MULTILATERAL TRANSPARENCY FOR SECURITIES MARKETS THROUGH DLT

David C. Donald[*] *and Mahdi H. Miraz*[**]

ABSTRACT

For decades, changing technology and policy choices have worked to fragment securities markets, rendering them so dark that neither ownership nor real-time price of securities are generally visible to all parties multilaterally. The policies in the U.S. National Market System and the EU Market in Financial Instruments Directive—together with universal adoption of the indirect holding system—have pushed Western securities markets into a corner from which escape to full transparency has seemed either impossible or prohibitively expensive. Although the reader has a right to skepticism given the exaggerated promises surrounding blockchain in recent years, we demonstrate in this paper that distributed ledger technology (DLT) contains the potential to convert fragmented securities markets back to multilateral transparency.

Leading markets generally lack transparency in two ways that derive from their basic structure: (1) multiple platforms on which trades in the same security are matched have separate bid/ask queues and are not consolidated in real time (fragmented pricing), and (2) high-speed transfers of securities are enabled by placing ownership of the securities in financial institutions, thus preventing transparent ownership (depository or street name ownership). The distributed nature of DLT allows multiple copies of the same pricing queue to be held simultaneously by a large number of order-matching platforms, curing the problem of fragmented pricing. This same distributed nature of DLT would allow the issuers of securities to be

---

[*] Professor, Faculty of Law, Chinese University of Hong Kong, Executive Director, Centre for Financial Regulation and Economic Development. The authors would like to thank Mathias Bock, Jochen Biedermann, Hongyi Chen, Joseph Lee, Keith Lui, Charles Mooney, Thrity Mukadam, Anthony So, Henry To, Padraig Walsh, and Kyle Walton for their comments on this paper. All errors and shortcomings remain our own.

[**] Postdoctoral Fellow, Centre for Financial Regulation and Economic Development, Chinese University of Hong Kong.

nodes in a DLT network, returning control over securities ownership and transfer to those issuers and thus, restoring transparent ownership through direct holding with the issuer.

A serious objection to DLT is that its latency is very high—with each Bitcoin blockchain transaction taking up to ten minutes. To remedy this, we first propose a private network without cumbersome proof-of-work cryptography. Second, we introduce into our model the quickly evolving technology of "lightning networks," which are advanced two-layer off-chain networks conducting high-speed transacting with only periodic memorialization in the permanent DLT network. Against the background of existing securities trading and settlement, this Article demonstrates that a DLT network could bring multilateral transparency and thus represent the next step in evolution for markets in their current configuration.

TABLE OF CONTENTS

INTRODUCTION

Shifting securities markets to a communication and registration framework of distributed ledger technology (DLT) [1] would allow markets to retain multilateral transparency despite their increasingly decentralized and fragmented nature.[2] The purpose of securities markets is to bring together buyers and sellers to contract for the sale and purchase of securities,[3] and then to facilitate the transfer of title and cash between those parties.[4] Since about 2000, the bid/ask queue of U.S. and European markets has been increasingly fragmented among various platforms.[5] And since about 1972, the indirect holding system has impeded transparent ownership of securities.[6] Use of a DLT network as the market's infrastructural spine could enable distribution of identical

1. MICHEL RAUCHS ET AL., DISTRIBUTED LEDGER TECHNOLOGY SYSTEMS: A CONCEPTUAL FRAMEWORK (Univ. of Cambridge Judge Bus. Sch. The Cambridge Centre for Alternative Finance Aug. 2018). We will use the definition of distributed leger technology developed by Rauchs et al. The definition is as follows: "A DLT system is a system of electronic records that (i) enables a network of independent participants to establish a consensus around (ii) the authoritative ordering of cryptographically-validated ('signed') transactions. These records are made (iii) persistent by replicating the data across multiple nodes, and (iv) tamper-evident by linking them by cryptographic hashes. (v) The shared result of the reconciliation/consensus process—the 'ledger'—serves as the authoritative version for these records." *Id.* at 23–24.

2. *See id.* at 45.

3. *See* ROBERT A. SCHWARTZ & RETO FRANCIONI, EQUITY MARKETS IN ACTION: THE FUNDAMENTALS OF LIQUIDITY, MARKET STRUCTURE & TRADING 82 (2004) ("The attributes of market quality include transparency, reliability, consolidation of the order flow, and easy access to a market, all of which directly affect liquidity and trading costs.").

4. Settlement is the "completion of a transaction, wherein the seller transfers securities or financial instruments to the buyer and the buyer transfers money to the seller." *See* BANK FOR INTERNATIONAL SETTLEMENTS, DELIVERY VERSUS PAYMENT IN SECURITIES SETTLEMENT SYSTEMS A2–6 (Sept. 9, 1992).

5. *See generally* FINANCIAL STABILITY BOARD, FSB REPORT ON MARKET FRAGMENTATION 23 (June 4, 2019); *see also* WALTER MATTLI, DARKNESS BY DESIGN: THE HIDDEN POWER IN GLOBAL CAPITAL MARKETS 108 (2019).

6. *See, e.g.*, PAUL MYNERS, REVIEW OF THE IMPEDIMENTS TO VOTING UK SHARES, REPORT TO THE SHAREHOLDER VOTING WORKING GROUP (2004).

information on pricing and holdings to market participants, restoring transparency of both the bid/ask queue and ownership.

The model sketched in this paper goes beyond what has been undertaken—or even proposed—to date, as it addresses all market functions from pricing to transfer of ownership. Despite the obvious attraction of using DLT to defragment market pricing, this has apparently not been proposed even by the team charged with defragmenting market price data under the U.S.'s multi-billion dollar Consolidated Audit Trail (CAT) project.[7] In securities settlements, with the exception of Australia,[8] DLT's announced use has been for marginal functions,[9] leaving core settlement operations unaffected.[10] During the

---

7. This project was launched in 2012 by the U.S. Securities and Exchange Commission (SEC). SEC Release No. 34-67457 (Aug. 1, 2012) 77 Fed. Reg. 45722 ("Consolidated Audit Trail"). Current information on the CAT is available at https://www.catnmsplan.com/.

8. The Australian Stock Exchange is currently rebuilding its Clearing House Electronic Subregister System (CHESS) on a platform of DLT, with a completion target of 2021. *See* AUSTRALIAN SECURITIES EXCHANGE, CHESS REPLACEMENT: NEW SCOPE AND IMPLEMENTATION PLAN, ASX (Apr., 2018), https://www.asx.com.au/documents/public-consultations/chess-replacement-new-scope-and-implementation-plan.pdf [https://perma.cc/3HJ6-YQXH].

9. For example, Enterprise Ethereum Alliance—a group of thirty tech giants such as Intel and Microsoft, banks such as J.P. Morgan Chase and Banco Santander as well as other organizations formed in early 2017—is working towards adaptation of Ethereum for the foreign exchange market for global currencies to facilitate the settlement layer of the trades. *See* Robert Hackett, *Big Business Giants From Microsoft to J.P. Morgan Are Getting Behind Ethereum*, FORTUNE, Feb. 28, 2017, https://fortune.com/2017/02/28/ethereum-jpmorgan-microsoft-alliance/?iid=recirc_f500profile-zone1 [https://perma.cc/S8JC-NJWR]; *see also* Mike Orcutt, *In 2019, blockchains will start to become boring*, MIT TECH. REV., Jan. 2, 2019, https://www.technologyreview.com/s/612687/in-2019-blockchains-will-start-to-become-boring/ [https://perma.cc/J73G-AQ2K].

10. This trend can be seen in the press surrounding the Nasdaq Stock Exchange, which in addition to be a securities exchange is also largely a purveyor of technology for securities exchanges. Early on, we have announcements of blockchain use that are highly marginal. *See* Martin Arnold & Nicole Bullock, *Nasdaq claims to break ground with blockchain-based share sale: Fight for bragging rights to 'first' transactions breaks out*, FIN. TIMES, LONDON (UK), Dec. 31, 2015, https://www.ft.com/content/eab49cc4-af18-11e5-b955-1a1d298b6250 [https://perma.cc/2M8G-SRWX]. One year later, vague statements about far-reaching change remain: Fredrik Sjöblom, *The Post-Trade Services Tipping Point*, NASDAQ MARKETINSITE (Dec. 14, 2016), https://www.nasdaq.com/articles/post-trade-services-tipping-point-2016-12-14 [https://perma.cc/7487-RWC7]. And most recently, we have the concrete sales of

years of blockchain's initial spike in popularity,[11] a number of institutions adopted marginal blockchain applications rationally exploiting the publicity bump that its adoption could provide.[12]

However, a large impediment to any significant change of market infrastructure is the ratio of cost to benefit. While there is encouragement to be drawn from the creation of the Investors' Exchange (IEX) to fight damaging high frequency trading techniques that exploited a fragmented market, major infrastructural shifts are far from the norm.[13] The existing, leading model for securities settlement enjoys great respect; replacing it with a relatively untested alternative would be unusual behavior for major market participants.[14] If the quantitative benefits to core system participants are viewed while ignoring negative externalities borne by others, the current arrangement

---

technology for special purpose platforms to settle trades in peripheral products (here, "settlement of tokenized assets and Singapore dollars"). *See* Johan Toll, *Blockchain Takes Major Step Forward with Collaborative Innovation in Singapore*, NASDAQ MARKETINSITE, (Aug. 24, 2018), https://www.nasdaq.com/articles/blockchain-takes-major-step-forward-with-collaborative-innovation-in-singapore-2018-08-0 [https://perma.cc/SK7L-WSR2]. For a discussion of the various initiatives as at the close of 2017, see John Manning, *How Stock Exchanges Are Utilising Blockchain Technology*, INT'L. BANKER, (Dec. 18, 2017), https://internationalbanker.com/brokerage/stock-exchanges-utilising-blockchain-technology/ [https://perma.cc/B9WK-SZS3]. In late 2018, Hong Kong Exchanges and Clearing Ltd. announced tangential use of blockchain technology in connection with its Stock Connect with mainland Chinese markets. *See* Alun John, *Hong Kong exchange turns to blockchain to open up Chinese shares*, REUTERS, Oct. 30, 2018, https://www.reuters.com/article/hkex-blockchain/hong-kong-exchange-turns-to-blockchain-to-open-up-chinese-shares-idUSL3N1XA4F1 [https://perma.cc/Y3FG-HEJ2].

11. Gartner plots blockchain as coming down from its height of hype in mid-2018, entering a stable slope toward eventual application. *See* Heather Pemberton Levy, *Understand how blockchain will evolve until 2030 and today's hype versus reality*, GARTNER, Oct. 16, 2018, https://www.gartner.com/smarterwithgartner/the-reality-of-blockchain/ [https://perma.cc/ZJ74-GABJ].

12. As RAUCHS ET AL., *supra* note 1, at 91 observed, "meaningful applications and implementations of DLT systems in production have rarely materialized to date: most projects are still in early trial or pilot phases . . . 'blockchain' and 'DLT' have become almost meaningless buzzwords that are—in many cases—mainly used for marketing and PR purposes . . ."

13. *See generally* SEC Release No. 34-78101 (June 23, 2016), 81 Fed. Reg. 41142 ("IEX Release").

14. This point is made very well by Michael Mainelli & Alistair Milne, *The Impact and Potential of blockchain on the Securities Transaction Lifecycle*, SWIFT INSTITUTE, 6, 22, 34–35 (2016).

and technology of securities settlement used on major markets is fast, secure, and profitable,[15] which itself nearly rules out a complete overhaul of existing systems with DLT.

An analysis that casts a wider net than immediate profits accruing to core market participants reveals the major flaws of fragmentation and indirect holding in contemporary securities markets. Pre- and post-trade price information has become fragmented as data transfer enabled the creation of alternative trade matching platforms. Regulations under the U.S. National Market System (NMS)[16] and the EU Market in Financial Instruments Directive (MiFID)[17] have legalized such platforms.[18] Because trades in securities listed on a major exchange in the United States or the European Union can be matched on any number of venues,

---

15. For 2017, the Depository Trust & Clearing Corporation reported 369 million securities transactions settled with a value of US $1.609 quadrillion, leading to revenues of US$1.06 billion, see THE DEPOSITORY TRUST & CLEARING CORPORATION, TURNING HEADWINDS INTO TAILWINDS: 2017 ANNUAL REPORT, DTCC, 64–66 (2017), http://www.dtcc.com/annuals/2017/static/pdfs/print-report.pdf [https://perma.cc/AL7W-727V].

16. *See* SEC Release No. 34-51808, "Regulation NMS," 70 Fed. Reg. 37496 (June 29, 2005) (Reg NMS), (codified at 17 C.F.R. § 242.600).

17. Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC, 2004 O.J. (L 145) (MiFID I). This framework has been replaced by a combination of a directive and regulation: Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU, 2014 O.J. (L 173) (MiFID II), and Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012, 2014 O.J. (L 173) (MiFIR). This is discussed in David C. Donald, *Bridging Finance Without Fragmentation: A Comparative Look at Market Connectivity in the US, Europe and Asia*, 16 EUR. BUS. ORG. L. REV. 173, 180–88 (2015) (hereinafter *Bridging Finance*).

18. In the United States, 17 C.F.R. § 242.600(b)(82) broadly defines the "trading center" matching platform to which Regulation NMS applies, no longer restricting such platforms to national securities exchanges: "Trading center means a national securities exchange or national securities association that operates an SRO trading facility, an alternative trading system, an exchange market maker, an OTC market maker, or any other broker or dealer that executes orders internally by trading as principal or crossing orders as agent." In the European Union (under current law) art. 1(19), (21)–(23) the monopoly of exchanges has been removed by creating the new general category of "multilateral system," and making "regulated markets," "multilateral trading facilities," and "organised trading facilities" subcategories under it.

pricing information for those securities has become widely fragmented.[19] Although sophisticated trade routing systems enable the largest broker-dealers to navigate this archipelago of platforms, less well-armed traders cannot.[20]

Market fragmentation is a significant flaw of the current market structure that concerns regulators at some level. The U.S. Securities and Exchange Commission (SEC) launched the multi-billion-dollar CAT infrastructure project in 2012 to repair this fragmentation at least for end-of-day data.[21] The EU rules provide for an analogous institution of a Consolidated Tape,[22] although it remains more of a hoped-for volunteer post than a realized project.[23]

Regulators have not publicly examined distributed ledger technology as a means of distributing pricing data. Instead, they have picked up the light mood found in companies adopting some token blockchain as publicity.[24] For example, the position taken by the European Securities and Markets Authority (ESMA)—which is in line with popular sentiment—is that DLT can offer efficiency, transparency, security, and reduced counterparty risk to markets.[25] The ESMA,

---

19. This follows from the nature of pricing in securities trading, which occurs when "bid" and "ask" orders are submitted to the matching platform by potential buyers and sellers of a given security, so that the order queue of each matching platform will generate its own price when orders match, triggering a trade.

20. The "arms race" of technology between broker-dealers has led to a significant reduction in the number of licensed broker dealers, as smaller competitors are no longer able to afford the technology necessary to remain competitive. For an analysis of this phenomenon, see David C. Donald, *From Block Lords to Blockchain: How Securities Dealers Make Markets*, 44 J. CORP. L. 1, 52–53 (2018) [hereinafter: *Block Lords*].

21. *See* 17 C.F.R. § 242.613(c)(7)(i)-(vii) (2016).

22. The name "consolidated tape" refers to the traditional "ticker tape" that showed execution or matching price for two orders throughout the 20th century. The purpose of this consolidated tape would be "make it easier for market participants to gain access to a consolidated view of trade transparency information that is available." MiFID II, Preamble 117.

23. Private persons may create a consolidated tape provider (CTP) and seek to be licensed to perform the under article 65 of MiFID II. No such CTPs have been registered as seeking authorization.

24. EUROPEAN SECURITIES AND MARKETS AUTHORITY (ESMA), THE DISTRIBUTED LEDGER TECHNOLOGY APPLIED TO SECURITIES MARKETS, ESMA Report, 26–33 (Feb. 7, 2017), https://www.esma.europa.eu/system/files_force/library/dlt_report_-_esma50-1121423017-285.pdf [https://perma.cc/DMK3-BTP2].

25. *See id.*

however, has not gone into detail on how this would occur or made any concrete proposal for implementation.[26]

Our model as presented in this paper would make order-matching venues nodes of a DLT network, so that the ledger protocol itself would replicate pre- and post-trade data on all copies of the ledger, restoring pricing information automatically.[27]

Beyond fragmentation of pricing information, the second major flaw in current market structure is its dependence on giving ownership of traded securities to a central placeholder—usually a central securities depository (CSD), but also sometimes the CSD's participant broker-dealers ("street names").[28] This damages property rights and rules out transparency, which impedes exercise of investor rights and triggers needless "corporate action" fees.[29] Shifting ownership to financial intermediaries has created the highly problematic "indirect holding system"[30] that gives financial intermediaries not only ownership of listed securities, but also the power—by booking securities to an account—to create securities for their accountholders, although those securities might never have been issued by the company against which they create a claim.[31] This power to "over-issue" securities arises because the

---

26. *See id.*

27. This is what the U.S. CAT is designed to do, and the European Union has also projected the creation of consolidated tapes ("CTs") in order to serve the same function, although there are no current plans to force industry to build one of volunteers are not forthcoming.

28. This is the industry standard that was expressed nearly twenty years ago in COMMITTEE ON PAYMENT AND SETTLEMENT SYSTEMS & TECHNICAL COMMITTEE OF THE INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS (CPSS-IOSCO), RECOMMENDATIONS FOR SECURITIES SETTLEMENT SYSTEMS, CPSS-IOSCO Joint Task Force on Securities Settlement Systems, Recommendation 6 at 13 (Nov. 2001) ("The costs and risks associated with owning and trading securities may be reduced considerably through immobilisation of physical securities, which involves concentrating the location of physical securities in a depository (or CSD)"), https://www.bis.org/cpmi/publ/d42.pdf [https://perma.cc/X9UN-NDLN].

29. *See* David C. Donald, *Heart of Darkness: The Problem at the Core of the U.S. Proxy System and its Solution*, 5 VA. L. & BUS. REV. 41, 49 (2011) (hereinafter *Darkness*).

30. This is defined in U.C.C. § 8 (NAT'L CONF. OF COMM'R ON UNIF. ST. L. 2017).

31. Under U.S. law, a booking to account by a securities intermediary actually creates property in security called a "security entitlement." *See* U.C.C. § 8-503 (2018). Investigation of the related problems were conducted by the U.S. Securities and Exchange Commission (SEC) before the Depository Trust Company (DTC) was created in 1972 and continued until the U.C.C. was restructured in the 1990s. For a

"securities" actually traded are the claims on account, requiring law to make the booking itself a security (an asset backed by the original security) albeit requiring the financial institution to eventually procure the underlying securities to back up the booking.[32] If we compare over-issue to the better known context of securitization, it would resemble a "synthetic securitization" in which the bonds issued are not backed by underlying mortgages.[33] However, in the indirect holding system, there is no need to label the arrangement as "synthetic." But in a DLT-based securities settlement system, ultimate evidence of ownership could remain on the books of the issuer, which would operate as a node in the DLT network, thus returning ownership of securities to the economic owners and returning full power over the creation of securities to their issuers.

A potential—and quite significant—drawback of decentralizing securities markets through DLT is the difficulty of retaining the central counter-party ("CCP") function, which can only operate by centering market risk and authority to debit and credit accounts on the CCP. Notably, the CCP contains the impact of a default only *after* it occurs. As CCPs absorb all counter-party risk in the market—yet are backed by all participants—they essentially are a network backing a single entity, responding in remedial fashion to default.[34]

In a DLT network, however, order-matching platforms are nodes with full information on the trading positions of market participants.

---

presentation of the history of these concerns and efforts, see Donald, *Darkness*, *supra* note 29, at 54–59. The problems of property and commercial law, discussed below, are examined in DOROTHEE EINSELE, WERTPAPIERRECHT ALS SCHULDRECHT: FUNKTIONSVERLUST VON EFFEKTENURKUNDEN IM INTERNATIONALEN RECHTSVERKEHR 144–149 (1995). More recent studies of disruption through complexity of intermediation and lack of transparency are MYNERS, *supra* note 6, and U.K. DEPARTMENT FOR BUSINESS, INNOVATION & SKILLS (BIS), EXPLORING THE INTERMEDIATED SHAREHOLDING MODEL, BIS Research Paper Number 261 (Jan. 14, 2016).

32. *See* U.C.C. § 8 (NAT'L CONF. OF COMM'R ON UNIF. ST. L. 2017).

33. In a synthetic securitization, contract rather than property rights protect the cash flows promised from the underlying mortgages, because "the securitization . . . [occurs] with the financial institution retaining legal ownership of the underlying loans (as opposed to a traditional structure, where the originator sells these loans to the securitization issuer in return for a payment financed by an issue of notes)." JASON H.P. KRAVITT & EDMUND PARKER, SECURITIZATION FIN. ASSETS § 20.03 (2019).

34. Froukelien Wendt, *Central Counterparties: Addressing Their Too Important to Fail Nature* 5, 10 (Int'l Monetary Fund, Working Paper 15/21, 2015).

Similar to a CCP on a derivatives exchange, much of the CCP risk management function could be made preventative. Matching venues within a DLT network could screen the cash, securities, and trading positions of participants before matching their orders, and throw any order backed by an unsatisfactory asset position to the back of the queue. This would provide preventative risk management for a purpose that CCPs on stock exchanges have only been able to provide remedial default containment.[35] If the latency of the screening could be reduced to an acceptable interval, such preventative measures would dramatically improve the risk management of securities trading and settlement systems.[36]

Moreover, incorporating matching venues within a DLT network could also address a new and growing fear arising from the current settlement model: excessive concentration of risk in central counterparties.[37] An additional risk-sharing and allocation agreement among broker-dealer nodes of the DLT network could contain risk not visible to the matching platform, much as done today in stock exchanges with the market backing the CCP.

This Article sets out in detail the reasons for and design of the model sketched in the preceding paragraphs. Part I examines the principal components of the currently dominant securities market structure, highlighting what works, how pricing information has been fragmented, what distorts property rights and transparency, and what could be improved most by a transition to DLT. Part I further explains the effects of multiple matching venues on pricing transparency, how transfers of ownership could be returned to issuers, and the operations of central counter-parties and our alternative that operates preventatively.

Part II then presents the key technical aspects of a DLT network with a focus on the applications most important to securities markets. Part III finally outlines the core operational concept of our proposed model using a DLT-based trade matching and settlement system, with a focus on the significant improvements and other changes it would bring. In particular, Part III explains that the DLT network would be

---

35. *See id.* at 15.

36. *See* Paul Lagneau-Ymonet & Angelo Riva, *Market Information as a Public Good: The Political Economy of the Revision of the Markets in Financial Instruments Directive (MiFID)*, in FINANCE: THE DISCREET REGULATOR—HOW FINANCIAL ACTIVITIES SHAPE & TRANSFORM THE WORLD 134, 15 (Isabelle Hault & Chrystelle Richard eds., 2012).

37. Wendt, *supra* note 34, at 4.

private/permissioned, giving authority over the booking of security ownership to issuer nodes, employing a "lightning network" to reduce latency, and making trade-matching nodes gatekeepers for preventative—rather than remedial—risk management. The final part of this Article summarizes the details of the model and concludes.

I. THE PRINCIPAL COMPONENTS OF SECURITIES MARKET INFRASTRUCTURE

A. THE DILEMMA OF FRAGMENTING MARKETS

Electronic trading has permitted the closing of trading floors and the multiplication of trade-matching venues, so that any platform connected to the market network can receive orders and match them.[38] This disintegration of matching venues was encouraged in the United States and the European Union as a way of pitting matching-venues against each other to reduce trading fees and stimulate innovation through competition.[39] Fees did decrease, and competition also spurred innovation, but the result was a fragmentation of liquidity among scattered pools and of pre- and post-trade information, fragmenting price discovery, and impeding effective market oversight.[40] Where traditional securities markets were dominated by a single matching platform at the close of the 20th century, order matching today is dispersed around tens, if not hundreds, of matching engines.[41]

Fragmentation of liquidity means that there are fewer bid and ask orders on any given sub-venue than there would be if all orders were concentrated on a single order-matching platform, like that of a traditional stock exchange.[42] Pre-trade information is the order book for a given matching venue, showing existing limit orders posted by market participants.[43] Post-trade information is the price at which a given trade is executed, essentially the ticker tape publicly visible on websites like

38. *See* SEC Release No. 34-51808, "Reg NMS," 70 Fed. Reg. 37496 (June 29, 2005) (Reg NMS), (codified at 17 C.F.R. § 242.600).

39. *See id.*

40. Xiangkang Yin, *A Comparison of Centralized and Fragmented Markets with Costly Search*, 60 J. FIN. 1567, 1584 (2005).

41. Donald, *Block Lords*, *supra* note 20, at 55.

42. Yin, *supra* note 40, at 1580.

43. SCHWARTZ & FRANCIONI, *supra* note 3, at 158.

Bloomberg.[44] When a single security is traded on fifty different order-matching venues, that number of bid/ask queues and execution prices will exist.[45] Although a participant's order routing tools are designed to seek out the venue with the most favorable price, modern market structure can hamper this.[46]

While leading market participants employ expensive technology to navigate the multiple platforms, gathering, comparing and consolidating the queues, this is not possible for all traders.[47] For smaller market participants that have neither the size nor the technology to trade simultaneously on many platforms, this reduces liquidity because it isolates pockets of buyers and sellers from each other, and tends to create uneven pricing for the same security on different matching platforms.[48] The arrangement thus leads to the kind of structured inequality of resources that Mattli has recently revealed in his political economy of the securities markets.[49]

The United States launched the CAT project in 2012 to tie back together the post-trade information—the price at which bid and ask orders are matched—generated at various venues.[50] This CAT is designed to provide only post-trade information to regulators,[51] and thus

---

44. *Id.* at 362–63.

45. As discussed above, securities market prices are "execution" prices at which a bid and ask order match. Each platform has its own order queue—indeed, that is the entire purpose of the platform's existence—so each platform creates its own execution price. If in the United States only the NYSE were to match orders, then its queue and execution price would be *the* market price, but when fifty platforms are matching orders in NYSE-listed securities, there will be fifty different execution prices, fifty different market prices.

46. *See, e.g.*, Guido Ferrarini, *Market Transparency and Best Execution: Bond Trading under MiFID*, *in* PERSP. IN COMPANY L. AND FIN. REG. 477, 479–80 (Michel Tison et al. eds., 2009).

47. Lagneau-Ymonet & Riva, *supra* note 36.

48. *Id.* at 150.

49. *See* MATTLI, *supra* note 5, at 106.

50. Joint Industry Plan; Notice of Filing of the National Market System Plan Governing the Consolidated Audit Trail, 81 Fed. Reg. 30614, 30615 (April 27, 2016) [hereinafter *81 Fed. Reg. 30614*].

51. *See id*. ("In performing their oversight responsibilities, regulators today must attempt to cobble together disparate data from a variety of existing information systems lacking in completeness, accuracy, accessibility, and/or timeliness—a model that neither supports the efficient aggregation of data from multiple trading venues nor yields the type of complete and accurate market activity data needed for robust market oversight.").

will not correct the problem of a market participant that might not have information on the bid-and-ask prices being considered at the countless different matching platforms in the market. Nevertheless, the CAT project team estimates $9 billion in sunk costs to put the CAT into operation for its first year.[52] The project's published plans make no mention of introducing DLT into the system.[53]

Using current technology, fragmentation results from creating multiple matching-venues that run their own order book and collect data using bid and ask orders from the various market participants trading on the matching-venue.[54] As explained in Part III.B, if each order-matching venue were to be a node in a DLT network and the data among the nodes were to be shared on a layer 2 "lightning network," the chain technology itself could ensure that each matching venue has the aggregate of all pre- and post-trade information in the network. The matching platforms, broker-dealers and the regulators would be nodes in the network with access to this information, and the problems arising from fragmentation would be eliminated.

B. INDIRECT HOLDING THROUGH CUSTODY ACCOUNTS

As securities markets collapsed under modern trading volumes in the late 1960s, introduction of the indirect holding system conquered the monumental administrative task of transferring millions of securities daily by simply ceasing most actual transfers of securities.[55] Securities certificates were immobilized in a CSD and registered in its name, the name of its nominee or that of an upper-level intermediary.[56] Although

52. The SROs that devised the CAT plan project "initial aggregate cost to the industry related to building and implementing the CAT would range from $3.2 billion to $3.6 billion. Estimated annual aggregate costs for the maintenance and enhancement of the CAT would range from $2.8 billion and $3.4 billion. Additionally, costs to retire existing systems would be approximately $2.6 billion." *81 Fed. Reg. 30614* at 30726-27.

53. Current information on the project is available at https://www.catnmsplan.com/.

54. *81 Fed. Reg. 30614* at 30672.

55. NATIONAL CONFERENCE OF COMMISSIONERS ON UNIFORM STATE LAWS, U.C.C. TEXT ART. 8 COMMISSIONERS, Westlaw (database updated Sept. 2017).

56. The history of this development is set forth in the following paragraphs, but it is useful to note at this time that the securities can be registered with the issuer (i) in the name of the CSD, (ii) in the name of a company that the CSD establishes as its nominee

the technique was already more than 100 years old when advocated in the 1970s,[57] it was—and remains—effective for the needs of fast transfer, albeit *what* is actually transferred remains open to interpretation.

The modern indirect holding system began in New York during the early 1970s.[58] Exchange-traded securities—then in paper form—were deposited in the vaults of the Depository Trust Company (DTC) and registered with the issuer in the name of its nominee, Cede & Co.,[59] which was henceforth the actual legal owner of these securities. Cede & Co. held them for one or another of its participating banks or securities dealers, and transferred claims on its accounts rather than the securities themselves.[60] When federal law in 1975[61] ordered the SEC to provide for "immobilization" of securities in depositories,[62] Cede & Co. came to legally own over 99 percent of U.S. listed securities,[63] with the remainder in its street names. This quickly became the global norm.[64]

---

expressly for this purpose, or (iii) in the name of a broker-dealer, in which case the broker-dealer would hold a segregated account for those securities at the CSD.

57. THEODOR HEINSIUS ET AL., DEPOTGESETZ: KOMMENTAR ZUM GESETZ ÜBER DIE VERWAHRUNG UND ANSCHAFFUNG VON WERTPAPIEREN § 5, margin no. 1 (1937).

58. The history of this major market structure change is set out in Donald, *Darkness*, *supra* note 29.

59. PETER NORMAN, PLUMBERS AND VISIONARIES: SECURITIES SETTLEMENT AND EUROPE'S FINANCIAL MARKET 41, 84 (2007); NATIONAL CONFERENCE OF COMMISSIONERS ON UNIFORM STATE LAWS, U.C.C TEXT ART. 8 COMMISSIONERS, Westlaw (database updated Sept. 2017).

60. EGON GUTTMAN, 28 MODERN SECURITIES TRANSFERS § 2:12, Westlaw (database updated May 2018).

61. *See* 15 U.S.C. § 78q–1(e) (2016). National system for clearance and settlement of securities transactions.

62. *See* Regulation of Clearing Agencies, 45 Fed. Reg. 41920 (June 23, 1980) (to be codified 17 C.F.R. pt. 21).

63. In 2004 DTCC's General Counsel Richard B. Nesson estimated that "somewhere north of 99%" of the depository-eligible securities in the United States were included within the DTCC system. *See* Interview with Richard B. Nesson, Managing Director and General Counsel, and Donald F. Donahue, COO, The Depository Trust & Clearing Corporation (Nov. 11, 2004), http://www.sechistorical.org/museum/programs/2004/[https://perma.cc/TA8K-YBT4].

64. The global norm for many aspects of financial market structure can be discerned from what is recommended by the high-level international bodies, the Bank for International Settlements and the Group of Thirty. The key components of the indirect holding system are recommended in both BANK FOR INTERNATIONAL SETTLEMENTS, COMMITTEE ON PAYMENT AND SETTLEMENT SYSTEMS: RECOMMENDATIONS FOR SECURITIES SETTLEMENT SYSTEMS (Nov. 2001),

Electronically agreeing that a securities dealer holds claim to something booked in a custody account is faster and simpler than actually transferring the securities. Actual transfer entails (i) delivery of the share certificate from seller to buyer, (ii) cancelling the share of seller and seller's entry in the register of shareholders, (iii) issuing the buyer a new certificate, and (iii) entering the buyer in the register of shareholders.[65] Such entry in the register of shareholders entitled the investing buyer to voting and dividend rights.[66] The indirect holding arrangement, by contrast, resembled a mille-feuille pyramid in which ownership held by the CSD and its top-level participants trickled down to lower-layer brokers and eventually to ultimate "beneficial owners," while claims of uncertain definitions from beneficial owners aspired upward to levels above.[67] Thus, although fast and secure, it is unclear exactly what is being held and transferred with such speed in this indirect holding system.

An investor's claim on a depository holding a security does not constitute a property right under conventional principles of law, which can have nasty consequences if the intermediary becomes insolvent.[68] In the United States, a property right for this essentially contractual relationship was created through amendment of the Uniform Commercial Code (UCC), article 8, in the form of the "security entitlement."[69] Outside of the United States, the assertion that a claim on a custodian—which is essentially *in personam*[70]—can be a property

---

[https://www.bis.org/cpmi/publ/d46.pdf https://perma.cc/9MY4-FDKR] and GROUP OF THIRTY, GLOBAL CLEARING AND SETTLEMENT: A PLAN OF ACTION (2003), https://group30.org/images/uploads/publications/G30_GlobalClearingSettlement.pdf [https://perma.cc/9DDA-V95Z].

65. *See* NATIONAL CONFERENCE OF COMMISSIONERS ON UNIFORM STATE LAWS, U.C.C. TEXT ART. 8 COMMISSIONERS, Westlaw (database updated Sept. 2017).

66. Under Delaware law, the relevant provision is § 219(c) DELAWARE GENERAL CORPORATION LAW ("The stock ledger shall be the only evidence as to who are the stockholders entitled by this section to examine the list required by this section or to vote in person or by proxy at any meeting of stockholders.") Dividends are paid out to the same list of stockholders.

67. *See* NATIONAL CONFERENCE OF COMMISSIONERS ON UNIFORM STATE LAWS, U.C.C. TEXT ART. 8 COMMISSIONERS, Westlaw (database updated Sept. 2017).

68. *See id.*

69. *See id.*

70. *See* DAVID C. DONALD, DER EINFLUSS DER WERTPAPIERABWICKLUNG AUF DIE AUSÜBUNG VON AKTIONÄRSRECHTEN, 124–25 (2008).

right has been strongly contested,[71] and a UNIDROIT convention drafted in the early 2000's to internationalize U.C.C., article 8, has never entered into force.[72]

The U.S. solution, however, has the disadvantage of allowing every booking to a custody account to create a security—analogous to a bank creating money by issuing credit—even if no securities exist to back up the booking.[73] This power to create securities is tied directly to the newly minted property right, for if a customer of a custodial bank actually owns a property interest thanks to a book-entry on account, there must really be a security behind that property interest, whether it has been issued or not.[74] As a result, if a securities dealer books 50,000 shares of IBM Corporation to a buyer's account, the buyer really owns the "security entitlement" on those shares, even if IBM never issued the shares.[75] That can lead to unwelcome consequences when the shares are voted or dividends on such shares are demanded.

---

71. These arguments with regard to German law are brought together by EINSELE, *supra* note 31, at 119. With regard to U.K law, see Roy Goode, *The Nature and Transfer of Rights Dematerialised in Immobilised Securities*, in The Future for the Global Securities Market: Legal and Regulatory Aspects 107, 120–27 (Obitah ed., 1996). On French law, see Didier R. Martin, *La théorie de la scripturalisation,* 20 ANS DE DÉMATÉRIALIZATION DES TITRES EN FRANCE 55, 61 (De Vauplane, ed. 2005). Under U.S. law, there is no problem of a property right because the U.C.C. has declared that the essentially *in personam* right against a securities custodian will be considered a property right. To advance a convention embodying this U.S. position, the International Institute for the Unification of Private Law (UNIDROIT) has assembled a guide showing how an account relationship could be understood to constitute a property right. *See* INTERNATIONAL INSTITUTE FOR THE UNIFICATION OF PRIVATE LAW, GUIDE ON INTERMEDIATED SECURITIES (2017), https://www.unidroit.org/instruments/capital-markets/legislative-guide (last visited Oct. 23, 2019).

72. The UNIDROIT Convention on Substantive Rules for Intermediated Securities requires ratification by three countries, but between completion in 2009 and this writing in 2019 only Bangladesh has agreed to ratification. *See* UNIDROIT, Status of the UNIDROIT Convention on Substantive Rules for Intermediated Securities (Oct. 9, 2009), https://www.unidroit.org/status (last visited Oct. 23, 2019).

73. U.C.C. § 8-501(b)(1) (AM. LAW INST. & NAT'L CONFERENCE OF COMMM'R ON STATE LAW 2018).

74. U.C.C. § 8-501 (AM. LAW INST. & NAT'L CONFERENCE OF COMM'R ON STATE LAW 2018).

75. As already stated, under § 8-504, the securities dealer will be responsible for procuring the securities created through booking, but if it cannot the problem of over-issue will affect the issuer of the securities, particularly when rights are exercised, such as during a shareholder meeting or a battle for corporate control.

Another major flaw of indirect holding is the famous problem that security holdings are completely opaque.[76] Issuers of listed securities might only have one name—that of Cede & Co. or another CSD in other markets—in their register of shareholders.[77] The actual shareholders become "beneficial owners" with a claim against their broker, which holds a claim against an upper-tier institution, which may hold a claim against a CSD.[78] The legal rights of shareholding belong only to the registered owner—in the United States, probably Cede & Co.—and must themselves be transferred or exercised in agency to govern the corporation.[79] The "beneficial owner" is visible only to the next level up.[80] Simple processes like calling annual shareholder meetings, voting at the same or making and accepting takeover offers become highly-convoluted affairs,[81] mediated by long chains of intermediaries for a "corporate action" fee.[82] These financial intermediaries, registered as shareholders, not only receive "corporate action" fees, but also enjoy the position of indispensable go-betweens in all shareholder relations because the issuers and the actual shareholders cannot communicate, or indeed, even have a legally binding relationship, without going through the intermediaries.[83]

Each of these problems arise from giving financial intermediaries primary ownership and control of listed securities—first through a depository relationship and then through the same arrangement even after securities certificates have been dematerialized. From the standpoint of data management, the indirect holding system makes the data about securities creation and ownership endogenous to the financial system.[84] The existence and control of such securities depends on neither their issuer nor the "owner" who ultimately paid for their purchase.[85] Transfer is fast and efficient because it remains endogenous

76. This is examined in detail in Donald, *Darkness*, *supra* note 29, at 59–62.

77. *See id.* at 62.

78. *Id.*

79. *See id.* at 49.

80. *See id.* at 73.

81. *See generally* MYNERS, *supra* note 6.

82. MICHAEL SIMMONS & ELAINE DALGLEISH, CORPORATE ACTIONS: A GUIDE TO SECURITIES EVENT MANAGEMENT 23–31 (2006).

83. *See id.* at 30.

84. This is an important conceptual aspect emphasized by RAUCH ET AL., *supra* note 1 in their analysis of DLT.

85. *See* Donald, *Darkness*, *supra* note 29, at 46.

to the financial system and under the control of financial intermediaries, with only records of secondary claims being communicated to outside parties such as issuers and investors.[86] The costs are a loss of property rights, the risk of over-issued "shadow" securities created by book entries and opacity of securities ownership.[87] The indirect holding system has since the 1970s made financial intermediaries indispensable parties in the creation, transfer, and ownership of securities by displacing issuers and alienating investors from direct ownership.[88]

As explained in Part III.C, *infra*, if securities are again evidenced only on the books of the issuer and thus exogenous to the financial system, transfer will be possible through booking of the security on the register of members, and investor ownership would be complete and transparent.[89]

C. Central Counter-Party Risk Containment

If all securities traded on a market are placed within a closed environment of accounts, as is done by the indirect holding system, it is possible to give one person the right to access and make transfers between those accounts.[90] If then all obligations arising from matched orders within the market are novated to insert that person as an obligor within every contact, it becomes the seller to every buyer, and the buyer from every seller, and thus a central counterparty.[91]

The CCP can use its authority to access all assets to reduce the risk of non-delivery or non-payment, and if such failure does occur, the CCP is in the position to absorb and slow the contagion effect of any such default.[92] The CCP's strength in this position is bolstered by the support that every clearing participant is obliged to give through funding a

86. *See id.* at 56–57.

87. *See id.* at 99.

88. *See id.* at 54.

89. As distinguished from a "security entitlement," which is a kind of claim backed by a security, a true uncertificated security exists only on one register and is transferred by simple debit and credit booking (essentially constituting delivery of the security). *See* Guttman, *supra* note 60, at 162–63.

90. *See* Ivana Ruffini and Robert S. Steigerwald, *OTC Derivatives—A Primer on Market Infrastructure and Regulatory Policy*, Fed. Res. Bank of Chicago Econ. Persp. 80-81 (2014).

91. *See id.*

92. Thorsten V. Koeppl and Cyril Monnet, The Emergence and Future of Central Counterparties 2 (Fed. Res. Bank of Phila., 2010).

guaranty reserve, contracting insurance, or both.[93] In derivatives exchanges, the CCP is further strengthened by receiving real time information about the trading positions and available assets of market participants and being vested with authority to demand that such market participants post margin payments or otherwise reduce their risk profile on the market.[94]

CCPs are understood to be one of the most useful components of the currently-dominant securities settlement framework.[95] They greatly reduce the systemic element of counter-party risk by inserting an entity backed by the entire market as every transaction's counterparty.[96] On a derivatives exchange, they also gather full information about market risk because they know both the trading and asset positions of their counterparties.[97] As is well known, the use of CCPs was the primary prescription to cabin risk from over-the-counter derivatives transactions, following the global financial crisis.[98] If CCPs have a disadvantage, it is that their concentration of risk in a single entity can make them "too big to fail."[99]

Real time reaction to information makes the CCP risk management on a derivatives market generally more comprehensive than in a stock

---

93. Robert R. Bliss and Robert S. Steigerwald, *Derivatives Clearing and Settlement: A Comparison of Central Counterparties and Alternative Structures*, FED. RES. BANK OF CHICAGO ECON. PERSP. 22 (2006).

94. On CCPs, see *id. See also* THORSTEN V. KOEPPL AND CYRIL MONNET, THE EMERGENCE AND FUTURE OF CENTRAL COUNTERPARTIES (Fed. Res. Bank of Phila., 2010); THORSTEN V. KOEPPL AND CYRIL MONNET, THE EMERGENCE AND FUTURE OF CENTRAL COUNTERPARTIES, Fed. Res. Bank of Phila. Working Paper 10-30 (2010), www.philadelphiafed.org/research-and-data/publications/workingpapers/; Marc Hollanders, *A look at the rapidly changing market infrastructure supporting the OTC derivatives markets*, 4 J. SEC. OPERATIONS & CUSTODY 7 (2011); Yee Cheng Loon and Zhaodong Ken Zhong, *The Impact of Central Clearing on Counterparty Risk, Liquidity, and Trading: Evidence from the Credit Default Swap Market*, 112 J. FIN. ECON. 91 (2014).

95. COMMITTEE ON PAYMENT AND SETTLEMENT SYSTEMS & TECHNICAL COMMITTEE OF THE INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS, *supra* note 28, at 12.

96. *See* Bliss, *supra* note 93, at 28.

97. *See id.* at 25–26.

98. GROUP OF THIRTY, FINANCIAL REFORM: A FRAMEWORK FOR FINANCIAL STABILITY, GROUP OF THIRTY REPORT (Jan. 15, 2009), http://group30.org/images/uploads/publications/G30_FinancialReformFrameworkFinStability.pdf [https://perma.cc/EC3L-M4YG].

99. WENDT, *supra* note 34, at 5.

market.[100] In a stock market, the CCP becomes the buyer to all sellers and the seller to all buyers, and then backs all positions through its access to securities and cash within the system and with the strength of the market's guaranty mechanism.[101] In the case where one or more market participants do not perform on a matched trade, the action taken is designed to absorb an existing shock.[102]

In a derivatives market, the CCP constantly scans the trading positions, paid-in margins and perhaps available collateral of system participants, asking them to adjust margin payments, and depending on the specifics of the system, even limit their trades according to position limits.[103] This additional CCP function is preventative in nature and manages risk much more effectively than unlimited access to resources in the case of a default.[104] Increasing the preventative functions of a CCP would thus augment its risk management capabilities.

We propose that the order-matching platforms within a DLT network be given both all information on bid/ask queues and the type of information available to a CCP on a derivatives market. As explained in Part III.D, *infra*, this would allow the order-matching platform to move orders to the back of the queue if it is not satisfied that the broker-dealer can perform. This preventative risk management could be coupled with a loss-sharing commitment among broker-dealers, similar to the network of remedial guaranty functions already used to support a CCP.[105] In this way, it should be possible for a trading and settlement system in the shape of a DLT network not only to reproduce, but also to improve upon the risk management functions of a CCP. To achieve the required latency, the protocol of the DLT network would use programmatically executed transactions (PETs), which are smart contract triggers for trade matching or rejection of orders to execute loss-sharing commitments.[106] This will be discussed in detail in Part III.C, *infra*.

---

100. Ruffini & Steigerwald, *supra* note 90, at 86.

101. *Id.* at 86.

102. *Id.*

103. *See* Richard Squire, *Clearing Houses as Equity Partitioning*, 99 CORNELL L. REV. 857, 857–70 (2014).

104. *See id.* at 858.

105. *See* Bliss & Steigerwald, *supra* note 93, at 27.

106. RAUCHS ET AL., *supra* note 1, at 37.

D. MULTILATERAL NETTING

Netting, also referred to as "clearing," is considered a core function of securities settlement systems, and is the reason why these systems are referred to as "clearing houses."[107] From the perspective of the securities settlement system's apex, multilateral netting of obligations owed among participants of the CSD can eliminate almost all transaction volume, dramatically reducing strain on the system's inner core.[108] In 2010, the last year that Depository Trust & Clearing Corporation (DTCC) publicly reported the netting efficiency of the National Securities Clearing Corporation (NSCC), it netted out 98 percent of transaction volume in each of the years from 2006 to 2010.[109] This steady ratio of 98 percent corresponds to the portion of the market's securities held through the accounts of upper-level participants in DTC, for it is the commonality of obligations among those participants that allow them to be netted.[110] Without common offsetting obligations between debtor and creditor, it is impossible to achieve an offset of what the two parties should pay to each other.[111] This commonality occurs because most of the securities traded on an exchange are held in the accounts of apex entities.[112] The netting of obligations among such apex entities holding direct accounts with DTC—and therefore accessible by NSCC—does not indicate an overall reduction of transaction costs per trade, but only a reduction of those transfer costs incurred at the system's apex.[113] Netting cannot eliminate the need for investors at the periphery of the system to make payments and deliver securities because such investors have no commonality of obligations with other such end users.

For example, if on a given trading day, a Boston resident enters into securities transactions with a profit of $1000, while a Miami resident enters into transactions with a profit of $1100, there is no commonality

---

107. *See* Squire, *supra* note 103, at 862.

108. *See id.* at 869.

109. THE DEPOSITORY TRUST & CLEARING CORPORATION (DTCC), SAILING TO THE END OF THE MAP: ANNUAL REPORT 2010, 25 (DTCC 2010), http://www.dtcc.com/~/media/Files/Downloads/About/Annual-Reports/2010_report.pdf [https://perma.cc/9RWM-BPDM].

110. *See id.* at 5.

111. *See* Squire, *supra* note 103, at 867.

112. *See* Donald, *Darkness*, *supra* note 29, at 61.

113. *See id.* at 15.

of obligation between them and it would never be a solution for the Miami resident to receive just $100 and the Boston resident zero, as the net of the credits held by each. This happens at the system apex because a handful of major broker-dealers have a very high share of the market, trade with each other, and settle these trades through accounts on the CSD.[114] This would likely not even be the case for the brokerages used by the respective investors in Boston and Miami, even if each of them engages Citibank as its global broker. At least for claims on account, the cash and securities due will have to be sorted out and passed down the pyramid to the end users. Assertions of the great efficiency of netting are thus possible because any security traded in the U.S. market has a 99 percent chance of being legally owned by Cede & Co. or one of DTC's core clearing participants.[115] However, the ability to net out the claims of top-level DTC participants in this way does not mean that the thousands of obligations passed up through the capillary system of correspondent arrangements from local houses during the same settlement cycle can be ignored.

As the accumulation of securities ownership in the omnibus accounts of apex intermediaries decreases, the volume of fungible obligations that can be netted out against each other also decreases.[116] If through a DLT network or otherwise, each investor owns securities directly, rather than having ownership moved to and bundled in a central group of intermediaries or the CSD's nominee, the percentage of nettable claims would be dramatically reduced. Commonality of obligations might remain only among institutions engaged in high-volume proprietary trading. Nevertheless, if a DLT network were to operate on a lightning network intraday, as explained in Part III.D, *infra*, it would be possible for market participants to go in and out of a position many times per day, with only the final position being settled. This would reduce transaction costs and could reduce the ultimate settlement volumes. Because ultimate attribution of claims to securities for transactions fully settled would be the result of such intraday transactions, the effect at closing would reduce system stress, albeit not through formal netting.

---

114. *See* THE DEPOSITORY TRUST & CLEARING CORPORATION (DTCC), *supra*, note 109, at 45.

115. *See id.* at 34.

116. *See id.* at 13.

II. THE TECHNOLOGY OF DISTRIBUTED LEDGERS

A. DIRECT ACCESS TO TRANSACTION DATA IN AN ADVERSARIAL ENVIRONMENT

Distributed digital ledger technology—such as blockchain—requires chronological records, i.e., "blocks" mathematically configured to behave in certain ways regarding requests for alteration, to be available on all the participating devices ("nodes") of its network, and operates in an adversarial environment. A DLT ecosystem is essentially a peer-to-peer ("P2P") network.[117] How new content is added to blocks depends on whether the ledger is "permissionless" or "permissioned."[118] In each case, however, read access to the data can be granted to all the participants, even in an adversarial environment.[119] Achieving this successfully requires a high level of security and privacy control, which is attained by cryptographic hashing algorithms as well as encryption mechanisms using a combination of private and public "keys."[120]

The possible contribution of DLT to securities clearing and settlement requires an examination of both the theoretical potential of blockchain technologies and their actual capabilities in the near term. Our analysis therefore entails scrutiny of three facets: (i) how cryptographic hash functions secure the chain, (ii) how the ledger architecture regulates its own modification, and (iii) how consensual control of the ledger occurs and affects operational latency.

---

117. RAUCHS ET AL., *supra* note 1, at 22 define an adversarial environment as being "characterised by the presence of malicious actors within a system or network, who undermine the system by using it in ways it was not intended for. The prototypical adversary in a DLT system is an entity that attempts to exploit the consensus rules to transfer assets without authorisation, censor others' transactions, or otherwise disrupt the network. Adversaries may operate inside or outside the system."

118. *See id.* at 30. In a permissionless blockchain ecosystem, anyone can freely and voluntarily join the network and have both write and read access—such occurs in Bitcoin's blockchain. In a permissioned blockchain ecosystem, joining the network is restricted to some specific nodes and write and read access is usually predetermined by a set of system rules.

119. *See id.* at 30.

120. *See id.* at 28.

B. THE CRYPTOGRAPHIC FUNCTION OF "HASHING" AMONG BLOCKS

The most prominent type of DLT is blockchain, which was initially developed for Bitcoin.[121] In its simplest form, a blockchain is a phalanx of digital blocks joined by interlocking encrypted data like the rings of a chain.[122] That is, each block contains the cryptographic "hash" of the previous block.[123] As a blockchain is used, blocks are added through transactions recorded as interlinked data, propagating the chain.[124] These transactions could be the creation of a new unit of value such as a Bitcoin, a transfer of such unit from one owner to another, or the memorialization of other information on the ledger. Because the ledger constituted by these blocks is held by each participating node, it is known as a distributed ledger network.[125]

Each chain has a "genesis block" marking the start of the chain.[126] The genesis block may contain instructions and procedures for the operation of the chain, which could be rules on the creation of new assets and establishing consensus, code for a smart contracts, or policy statements.[127] In a ledger serving a securities trading and settlement system, the genesis block could contain rules and procedures on verification of available funds and securities, how to match trades within the system, requirements for consensus on settlement, performance of payment, and transfer of title to securities.

This Article recommends use of a private/permissioned ledger for trading and settlement, which would give extensive control to the largest and most influential market participants—a feature that some readers

---

121. In cryptography, keys are used to encrypt and decrypt data. In asymmetric cryptography—also commonly known as public key cryptography—a mathematically bound pair of private-public keys are used. A public key is used to encrypt data while a private key is used to decrypt the encrypted data. These keys are simply non-identical very large numbers which are mathematically paired together. Another important use of these keys is digitally signing and verifying documents. In blockchain systems, public keys are often used as the account (more commonly known as wallet) identifier—analogous to any bank account number. Such use of public key requires the key to be unique within the blockchain network. *See id.* at 28.

122. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN (2008), https://bitcoin.org/bitcoin.pdf [https://perma.cc/VSG3-EYD7].

123. Mainelli & Milne, *supra* note 14, at 3.

124. Satoshi, *supra* note 122, at 2.

125. Mainelli & Milne, *supra* note 14, at 3.

126. *See id.*

127. *See id.*

may see as undesirable. To that end, it is important to understand the operation of public and permissionless ledgers and the problems that they present. Modification of the ledger is self-regulating in a public and permissionless system—like Bitcoin—because blocks are added to the chain by completing a "Proof-of-Work" ("PoW") mathematical puzzle that requires considerable computing power and "hashes" the digital ledger of transactions against alternation.[128] In Bitcoin, completing a PoW puzzle is referred to as "mining"[129] and originated with Adam Back's HashCash.[130] The rules for Bitcoin's blockchain provide that a transaction initiated by a node broadcasting it to the blockchain network is only complete upon validation by the other nodes.[131] These transactions remain "unconfirmed" and must be assembled with other unconfirmed transactions into a "candidate block," which itself must be validated through PoW and consensus.[132]

---

128. *See* RAUCHS ET AL., *supra* note 1, at 55.

129. Satoshi, *supra* note 122, at 3.

130. Mining in Bitcoin BC is analogous to mining of gold or any other valuables. In Bitcoin BC ecosystems, supply of new Bitcoin (BTC) is only made available by mining. Mining also serves as an incentive, more commonly known as block reward, for the miners (participating nodes). As of July 2018, 17.1 million of BTC has been mined which is 81.43 percent of the planned cap of maximum 21 million. It may seem that if 81.43 percent of BTC is mined in nine years since BTC started its journey in 2009, the remaining of the BTCs will be mined within a very short while. However, this is not going to be the case as the block reward is halved every 210,000 blocks, which is approximately every four years. In 2009, the initial block reward was fifty BTC, which fell to 12.5 BTC by 2017, and it is estimated this will be further halved by 2020, so that the remaining 18.57 percent of BTC would be mined around 2140. *See* Jamie Redman, *80% of the 21 Million Bitcoins Have Been Mined Into Existence*, BITCOIN.COM NEWS (Apr. 27, 2018), https://news.bitcoin.com/80-of-the-21-million-bitcoins-have-been-mined-into-existence/ [https://perma.cc/832H-Y3QP]. Once all 21 billion coins are mined, the Bitcoin BC ecosystem could run solely on transaction fees and adopt Proof-of-Stake ("PoS"). There is debate whether mining will remain economically beneficial enough for mining to continue, the rising price of BTC due to "controlled supply" is one of the major grounds why it may continue.

131. Adam Back, *Hashcash—A Denial of Service Counter-Measure* (Aug. 1, 2002), http://www.hashcash.org/papers/hashcash.pdf [https://perma.cc/4PB6-R2TC].

132. Mahdi H. Miraz & David C. Donald, *Application of Blockchain in Booking and Registration Systems of Securities Exchanges in* INTERNATIONAL CONFERENCE ON COMPUTING, ELECTRONICS & COMMUNICATIONS ENGINEERING, ICCECE 35–40 (Aug. 2018), available at https://ieeexplore.ieee.org/document/8658726 [hereinafter *Application of Blockchain*].

The life-cycle of a transaction in a public and permissionless ledger has several phases, including transaction formation, broadcast to the network, verification and validation through PoW, and consensus.[133] In a DLT network facilitating a securities market, examples of transaction formation include a broker-dealer placing an order to buy or sell a security, or an issuer creating a new share of stock. In a public network, these would be broadcasting to peer nodes, which would verify and validate the same, adding them to a pool of unconfirmed transactions. Unconfirmed transactions would then be selected for incorporation into a candidate block for solution of the PoW puzzle. Once the puzzle is completed, the block would be sealed and broadcasted for validation.[134] Consensus of the nodes over validation would add the block to the existing chain. Rauchs *et al.* refer to this process using the phases of transaction, log, record, journal and ledger, in which the "record" stage is equivalent to an unconfirmed transaction and the "journal" is the set of records found in a candidate block.[135] Thus, in a public and permissionless ledger, all participating nodes would have a certain unacceptable amount of control over both a broker-dealer's trading choices and the existence of securities created by a given issuer.[136]

Permissionless ledgers are self-sufficient; they do not require an active administrator to protect against unauthorized alteration because the embedded encryption and connected validation process serve this control function autonomously.[137] This could provide desired neutrality of administration in a securities market but would almost certainly lead to unacceptable levels of latency. A PoW puzzle requires calculating the hash of the block at a difficulty level set by the historical speed of solution, which at mid-2018 was approximately 10 minutes for the Bitcoin blockchain.[138] This high latency means that a given node itself will have a very limited scale during a given time frame, leading to a restricted scalability for the entire network. For a securities market in which 3,000 different assets might be traded at a given moment, this would likely be a fatal defect.

---

133. *See* RAUCHS ET AL., *supra* note 1, at 19.

134. *Id.* at 60–65.

135. *Id.*

136. *See id.* at 74.

137. *See id.* at 68.

138. Mahdi H. Miraz & David C. Donald, *Atomic Cross-chain Swaps: Development, Trajectory and Potential of Non-monetary Digital Token Swap Facilities*, 3 ANN. OF EMERG. TECH. IN COMP. (AETIC) 42, 42–43 (2019) [hereinafter *Atomic Swap*].

Capped transaction throughput, resulting from the decentralized PoW and consensus approach, remains at the center of all concerns associated with scalability of blockchain based applications. A further significant disadvantage of permissionless DLT is the way PoW is forced to evolve within its environment, particularly by the adjustment of the difficulty level.[139] For example, Bitcoin's transaction capacity is seven per second on average, while that of Ethereum is 15 per second; Ripple's capacity in this regard is much higher, at 1500 transactions per second, but still much lower than Visa, which can process 24,000 transactions per second on average.[140] That said, choices by nodes acting in a given ledger according to fees or other incentives could cause an unconfirmed transaction to take several days to complete settlement.[141] Traffic also significantly affects latency.[142] The queue time in Ethereum is thus exponentially increasing due to mushrooming use from Initial

139. The Bitcoin mining difficulty level is a measure of how difficult the PoW puzzle actually is—to find a SHA-256 hash of a block's header. To claim successful completion of the PoW puzzle and be accepted by the Bitcoin ecosystem, the calculated hash must be equal to or lower than the target. The mining difficulty is adjusted after every 2016 blocks, i.e. a duration of roughly two weeks, using the following simplified version of the formula:

$$New\ Difficulty\ Level = Current\ Difficulty\ Level * \left(\frac{Expected\ Average\ Time}{Actual\ Average\ Time}\right)$$

Thus the ratio resulting in $\left(\frac{Expected\ Average\ Time}{Actual\ Average\ Time}\right)$ determines the difficulty level of PoW puzzles for the next 2016 blocks created. If greater than 1, the difficulty level increases, and if less it decreases. If the difficulty level decreases or remains the same throughout the life cycle of the Bitcoin ecosystem, blocks will be created faster because of the increase in computing power (pursuant to Moore's Law, and perhaps even a super-accelerated leap through quantum computing) and a larger number of miners and their collaboration in pools. The system must compensate by raising the PoW difficulty level in order to dampen the block generation rate. The maintenance of an average block generation rate has protected the Bitcoin ecosystem from attacks by malicious miners. Any block that does not meet the set PoW target will be rejected by nodes in the network and become worthless.

140. *See* Richard MacManus, *Blockchain Speeds & The Scalability Debate*, BLOCKSPLAIN (Feb. 28, 2018), https://blocksplain.com/2018/02/28/transaction-speeds/ [https://perma.cc/D4HF-XVBE].

141. Miraz & Donald, *Atomic Swap*, *supra* 138, at 43.

142. *Id.* at 42–43.

Coin Offerings (ICOs), Decentralised Autonomous Organization (DAOs), and Decentralised Apps (DApps).[143]

This high latency arising from calculation of the hashed block header is perhaps the largest drawback for financial market use.[144] The hashed block header, however, cannot be eliminated because it is the backbone of the PoW security model.[145] An alternative approach is Proof-of-Stake ("PoS"), which is used in permissioned (private) ledgers.[146] Unlike PoW, a chain using PoS assigns certain nodes the authority to add to the ledger based on proportionate holding of assets in the chain.[147] For a private/permissioned ledger, it is also possible to assign authority to given nodes in mutual agreement or by means of other authority.[148] Such nodes would have power to create blocks on the ledger. The blocks in a permissioned system using PoS or another model are linked with an agreed pattern hashing, rather than through hashing set at a level of difficulty.[149] PoS offers lower latency, allowing more transactions to be processed per unit of time, but also requires a closed network, which shifts responsibility for the network's security back to a system rules framework agreed among participants and away from automatically executing code. As will be discussed in more detail in Part III, we recommend use of a private/permissioned network because it offers the low latency necessary to match and settle securities transactions.

---

143. Ethereum is not just a cryptocurrency network; rather it offers blockchain as a service. Individuals or organizations aiming to develop their own blockchain or smart contract-based applications may use the Ethereum blockchain platform to run their applications, which includes launching ICOs or other DApps.

144. *See* Slimcoin, *A Peer-to-Peer Crypto-Currency with Proof-of-Burn*, SLIMCOIN WHITE PAPER (May 17, 2014), https://github.com/slimcoin-project/slimcoin-project.github.io/raw/master/whitepaperSLM.pdf [https://perma.cc/YGV9-PT7A].

145. *See id.*

146. *See id.*

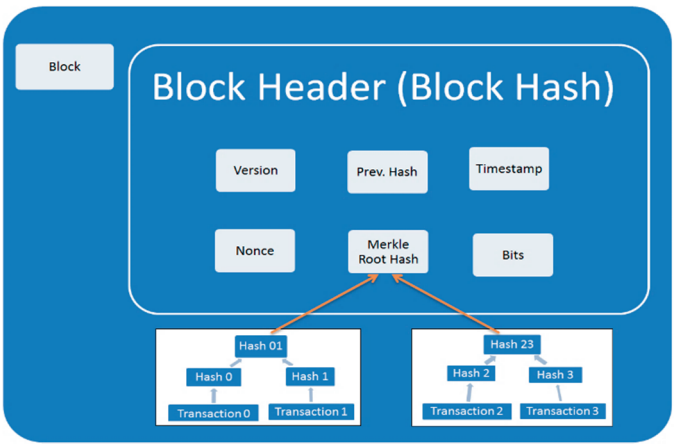
147. Another emerging variant to these predominant approaches, which is considered not only to be supportive of the green-computing movement but also having substantial economic contributions towards the adopting cryptocurrency, is the "Proof-of-Burn" ("PoB") *modus operandi* introduced by Iain Stewart. *See id.* Unlike PoW, the computational cost of solving the mathematical puzzle is replaced in PoB with a solely monetarily expensive task, i.e., to "burn" some coins by transferring them to an address where they are blocked and cannot be spent.

148. Slimcoin, *supra* note 144.

149. *See id.*

To grasp the network linkage among blocks, their durability against unintended replication, and the activity performed in PoW, a look at a block's internal components is useful. As mentioned above, the genesis block is quite different from the others, as it can contain smart contracts specifying rules for node verification and validation or for the routine operations of the ledger ecosystem. As shown in Figure 3.1 below, a block contains a version number (4 bytes), a hash of the previous block (256 bytes), a timestamp in seconds (4 bytes), a "nonce"—which is a one-time password or key (4 bytes), the current difficulty level (4 bytes)—and the Merkle Root hash of transactions.

Figure 3.1



The hash function is based on an algorithm that accepts any size data input, but is restricted to a fixed size output known as the "hash value" or simply the "hash."[150] Creating a hash is simple, but deciphering the key input factors is impossible even if the algorithm is known.[151] A hash is non-reversible because changing even a single bit of

150. Bitcoin blockchain uses a hashing technique called SHA-256 of the SHA-2 family whereas Ethereum blockchain uses Keccak-256, both of which produce digests (hash value) of 256 bits. RIPEMD160 is a cryptographic hash function that produces 160 bit of hashes. Bitcoin uses both RIPEMD160 and SHA-256 simultaneously. To further tighten the security threshold, hashing function is used twice in Bitcoin blockchain. For addresses, Bitcoin blockchain uses RIPEMD160 (SHA-256 (key)) and for other purposes blockchain uses SHA-256 (SHA-256 (data)). The use of RIPEMD160 enables the addresses to be shorter, as it generates the shortest hashes whose uniqueness is still guaranteed to an adequate degree.

151. *See* Slimcoin, *supra* note 144.

the input data produces a completely different hash.[152] Hash values are also known as "message digests" or simply "digests."

Such application of hashing techniques protects the chain against falsification or alternation even without a monitoring authority.[153] Once the genesis block and other protocols are written, the structure of a permissionless DLT network alone ensures that bookings on the ledger are authorized.[154]

Ledgers use a Merkle Tree arrangement[155] so that the blocks need not preserve full individual hashes of each transaction because information in the common "root" joining the "leaves" is a sufficient marker, which substantially reduces file size.[156] The Merkle "root" is a hash, efficiently constructed from the contributions of all the hashes included in any particular block of the chain.[157] Figure 3.2 below exemplifies a Merkel Tree as used in Bitcoin blockchain.

---

152. For this demonstration, we used an online Hash Generator that facilitates SHA-2 (256 bit) Hashing using UTF8 Character Encoding which is freely available at https://dev-tips.org/Generators/Hash/SHA256. In the instance of a small change in the original text–such as "a" instead of "o"–the pattern of the hash changes significantly, e.g., "securities depositary" produces a digest of "AC9D1A02E7E1224A75 A1C6FD800399A22BF9878E70D4373FF0770DAC34D50380" while "securities depository" generates an output of "4BBA914A3AB03BACC3556A2B476E 87DD7D1D7F1912A58CEE683E08826D49F900." Hash inputs are also case sensitive, e.g., "securities depositary" generates a digest of "92D6EEBDC1ED6B56302323A1F FFB3088414146E9F07D98591FFB8F6E75411AC4" while securities depository results in a digest of "6D2D92614BAA776F8CEC63C26DD97B28AC65B02B74048881956 CFFAAC84399DC." When upper case "A" and "O" are replaced with lower case "a" and "o," the hash becomes completely different. The hash of a hash produces a completely new hash, e.g., "The quick brown fox jumps over the lazy dog" produces a digest of "D7A8FBB307D7809469CA9ABCB0082E4F8D5651E46D3CDB762D02D0 BF37C9E592" which, if used as an input, produces another digest of "616687DF387FAEFAB7E9800C3CBDC97C1701A82622E9939BF59A2BD98319AC 6A." The outputs (i.e., hashes) in all six cases are of same length regardless of the size of the inputs (i.e., the original texts). In this case, the length is 64 hexadecimal digits equivalent to 256 binary bits.

153. RALPH C. MERKLE, PROTOCOLS FOR PUBLIC KEY CRYPTOSYSTEMS, IEEE SYMP. ON SEC. AND PRIVACY 122, 126 (1980).

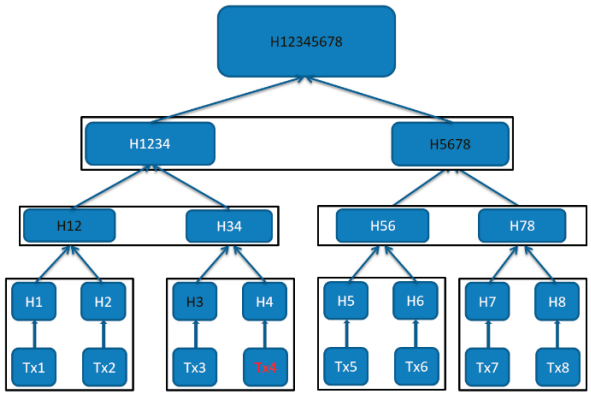
154. *See id.*

155. *See id.*

156. *See id.* at 125–27, 129.

157. *See id.* at 124–27.

Figure 3.2



Whether a ledger is permissionless or permissioned, the hashing protects the ledger's data: if a verifier addressing the scenario depicted in Figure 3.2 wants to ensure that a third party has not tampered with transaction Tx4, he may request the server to confirm that the transaction Tx4 has been included in the block. The server returns the hash of Tx3 which is H3 as well as H12, H5678 and H12345678. Verifier calculates: H4 from Tx4, then H34 from given H3 and calculated H4, then H1234 from given H12 and calculated H34, and finally H12345678 from given H5678 and calculated H1234. If the given and the calculated versions of the Merkle Root (H12345678) are the same, the transaction has been properly included in the block.[158] This arrangement also enables participants to calculate the Merkle Root and any intermediate nodes to verify that transmitted data has not been altered, allowing efficient verification for audit purposes without having to examine the actual records behind the root.[159] Because this technique is also present in permissioned ledgers, data integrity and immutability for such arrangements would not depend alone on enforced authority and data access rules among the permissioned parties.[160] This process is more secure than current market infrastructure designs.[161]

158. *See id.* at 125, 128.

159. *See id.* at 124, 132.

160. European Securities and Markets Authority (ESMA), *The Distributed Ledger Technology Applied to Securities Markets*, 2017 ESMA REPORT 1, 4, 6.

161. *See* Shashank Bilonia, *Blockchain Technology—Unfolding the Technology Behind Bitcoins*, EDUREKA!, https://www.edureka.co/blog/blockchain-technology/ [https://perma.cc/APM8-TR9W] (last updated May 22, 2019).

C. Data Decentralization Through Distribution

The standard settlement system of a major securities exchange is highly centralized, concentrating a very large portion of the securities traded within a network of accounts held by a CSD and giving the CCP information from and power over those accounts.[162] Indeed, the first word of these two key institutions is *central*. The primary advantages of the decentralization found in a DLT network are (1) replication of data identically in all copies of the ledger, (2) consensus governance, and (3) no single point of failure (SPF) vulnerability.[163] As central counterparties are perhaps the strongest component of existing systems and decentralization is a key feature of any DLT system, any evaluation of DLT for securities settlement must understand how the distributed nature of a DLT network can still aggregate overall data as if it were centralized.[164]

A DLT network is defined by how its nodes interact.[165] The blockchain network, for example, clusters together various technologies: (a) cryptographic algorithms, (b) distributed network, and (c) programs such as the blockchain protocol.[166] Each network node computing device will hold its own copy of the entire ledger and will interact with and contribute to conserving the consistency of the chain using this cluster of technologies.[167]

Cryptographic algorithms predetermine much of a ledger's operation.[168] Transactions are initiated with a private/public pair of cryptographic keys, and each public key—which is known throughout the network—will correspond to only one private key.[169] A transacting node digitally "signs" the transaction by encrypting it with its private key, which can then be decrypted by other nodes using the corresponding public key.[170] As De Filippi points out, this resembles an

---

162. European Securities and Markets Authority (ESMA), *The Distributed Ledger Technology Applied to Securities Markets*, 2017 ESMA Report 1, 4, 6.

163. *See id.* at 4.

164. *See* Bilonia, *supra* note 161.

165. *See id.*

166. *See id.*

167. *See id.*

168. *See id.*

169. Primavera De Filippi & Aaron Wright, Blockchain and the Law: The Rule of Code 20–21 (2018).

170. *See id.* at 14–15.

email system in which each user has a public identity—their email address—and a private password to open, write and read email.[171] The main difference is that in a DLT network, the public key is locked to the private key mathematically so that one cannot be changed without changing the other.[172] This allows independent action by each network node and would be the same in both permissionless and permissioned networks.

Distribution enables the consensus aspect of network operation.[173] Once a transaction is accepted upon application of the public key, it is considered "unconfirmed" and queued as a candidate for addition to the ledger.[174] At this point, if the ledger is permissionless, miners compete to solve the PoW puzzle by adding the nonce in calculating the hash value of the block header that matches the current target value, as explained above. When the puzzle is solved, the block is broadcasted to the network. [175] Other nodes then validate the transaction by recalculating the hash, adding the block to their copy of the ledger.[176] This consensus control—like other systems dependent on majority control[177]—remains secure as long as the share of the computation power of the honest nodes exceeds the share of computation power of the dishonest nodes. If a dishonest node has a minority position, the other nodes will not accept its solution of the PoW with altered data if the solution does not match the unconfirmed transactions they have on record. Thus, consensus building according to this preconfigured autonomous nature of a DLT model could force the system into default. In a permissioned network with assigned authorities to specific nodes, the problem would be reduced. Of course, the extra-protocol problem of consensus in assigning these authorities at the time of system creation would still exist, as it does in any federated system with assigned powers.

---

171. *See id.* at 24, 29, 31, 74.

172. *See id.* at 21–22.

173. *See* Bilonia, *supra* note 161.

174. *See id.*

175. *See* DE FILIPPI et al., *supra* note 169 at 25.

176. *See id.*

177. Majority control of stock corporations, which appears simple at first glance, is subject to every kind of strategic gaming and abuse, which has led to legal remedies such as the unfair prejudice action under U.K. law and the action applying a controlling shareholder's fiduciary duty under U.S. Delaware law.

The above procedures secure public or permissionless networks like Bitcoin, Ethereum, Factom, and Blockstream.[178] A private or permissioned network—like the proprietary systems currently used for clearing and settlement—would allow only "trusted" nodes to read and write on the ledger.[179] Permission can be granted at different levels, so that different types of nodes have authority to read differing types of information and only certain nodes have authority to write on the ledger.

Private blockchain ecosystems are already operated by Eris Industries, Blockstack, Multichain, and Chain.[180] In 2015, Chain joined NASDAQ in a partnership to allow the secure issue and transfer of shares in privately-held companies on a blockchain ecosystem, dubbed NASDAQ Private Market (NPM).[181] The main difference between this system and the traditional securities settlement model is that power is distributed to key system participants as opposed to being aggregated in the CCP.[182] The model we propose in Part III would give diverging types of authority to three different classes of system participants: order-matching platforms, broker-dealers, and issuers of securities.

178. *See* DE FILIPPI et al., *supra* note 169 at 31.

179. *See* Laura Shin, *Nasdaq Selects Bitcoin Startup Chain To Run Pilot in Private Market Arm*, FORBES, June 24, 2015, https://www.forbes.com/sites/laurashin/2015/06/24/nasdaq-selects-bitcoin-startup-chain-to-run-pilot-in-private-market-arm/#664f473583d5 [https://perma.cc/F3FG-7J7E]; *see also* John McCrank, *Nasdaq Partners with Chain To Bring Blockchain To Private Market*, REUTERS, June 24, 2015, https://www.reuters.com/article/nasdaq-blockchain/nasdaq-partners-with-chain-to-bring-blockchain-to-private-market-idUSL1N0Z92I720150624 [https://perma.cc/P7AF-FQJL].

180. *See* Miraz & Donald, *Application of Blockchain*, *supra* note 132, at 38.

181. *See* Shin, *supra* note 179.

182. Although a CCP is in all instances a corporation backed by all market participants with capacity to hold accounts in the CSD and accept transfers between those accounts as executed by the CCP, the corporation is much like a placeholder for a network of these participants because they provide guarantees in various ways for its debts. With the model we recommend, the network does not require a placeholder corporate body to unite it because it is held robustly in place by the distributed ledger.

D. REDUCING LATENCY WITH LIGHTNING NETWORKS

In Part II.C, we explained that a private/permissioned network can achieve more favorable latency than a public/permissionless one. Nevertheless, even a private DLT network would be too slow to compete with current data transmission on securities exchanges.[183] This is the result of two architectural limitations that a number of people have attempted to overcome—a lack of interoperability and a lack of scalability.[184] Thus, the initial blockchain technology developed as a by-product of Bitcoin [185] has seen a significant rise in multifaceted domains.[186]

In the challenge to achieve interoperability between different cryptocurrencies or colored coins, the recent development of variant "atomic swap" mechanisms hold great potential. The term "atomic" is commonly used in database system terminologies to indicate a binary output, meaning that the action will happen either entirely or not at all. [187] "Atomic swaps" in blockchain ecosystems are direct P2P exchanges of crypto assets between two parties in which the swap process occurs at a binary level governed by coding—such as cryptographically powered smart contract technology—rather than any centralized intermediaries. [188] Atomic swaps eliminate the need for legacy exchanges, as there remains no risk of default—both the parties have full control and ownership of the crypto assets dedicated to the transaction until it takes place, and then transfer to the counterparty occurs fully and automatically.[189] Viewed legally, performance is not subject to any kind of condition or unwinding.[190]

Depending on the architecture of the DLT ecosystem and the location of the interim transaction, atomic swaps can be "on-chain" or "off-chain."[191] The swap is "on-chain" if the interacting DLT systems

---

183. *See* Miraz & Donald, *Atomic Swap*, *supra* note 138, at 48.
184. *Id.*
185. *Id.* at 43.
186. *Id.*
187. *Id.* at 44.
188. *Id*.
189. *Id.* at 45.
190. *Id.*
191. *Awesome-lightning-network*, GITHUB (last visited Oct. 23, 2019), https://github.com/bcongdon/awesome-lightning-network

are technologically homogeneous.[192] "Off-chain" swaps have been made possible by the recent invention of "lightning networks" that are able to join technologically heterogeneous DLT systems.[193] An off-chain swap using a lightning network occurs away from the base chains on a completely separate layer known as "second layer" or "layer 2."[194]

Lightning network technologies were developed for general application in 2017 and hold the potential to reduce latency, thereby allowing DLT to provide its inherent benefits to the user at greater speed and scalability.[195] The adjective "lightning" is used because data can be transferred instantaneously between nodes on a second channel layer that is not subjected to a consensus process.[196] This second layer is powered by a Hashed Timelock Contract (HTLC)-based smart contract, enabling bi-directional payment channels built on top of the base layer of DLT.[197] Nodes of homogeneous DLTs can also benefit from the speed of lightning networks.[198] At its simplest, this use occurs when two parties—nodes in DLT networks—agree on a shared private key for the swap, and the swap of their crypto assets will take place on a second layer only if the counterparties use the same private key.[199]

A HTLC backing of the lightning network enables bi-directional payment channels through a second layer built on top of the base DLT layer.[200] Lightning network transactions occur through "matching" of shared keys, rather than through a classic consensus approach. Thus, along with offloading the transactions from base channel, lightning networks enable instantaneous transfers of assets with near-zero

---

[https://perma.cc/S4YH-P9LJ] (detailing a complete and updated list of lightning network updates). To date, the three major implementations of such lightning networks are: Blockstream's "c-lightning" implementation in C, Lightning Labs' Golang's implementation of "Lightning Network Daemon (LND)," and ACINQ's Scala implementation of "eclair." Ethereum's Raiden Network is also an example of off-chain scaling similar to a lightning network.

192. *See* Miraz & Donald, *Atomic Swap*, *supra* note 138, at 46.

193. *See id.* at 48.

194. *See id.* at 46.

195. *See id.* at 47.

196. *See id.* at 46.

197. *Id.*

198. Mahdi H. Miraz & David C. Donald, *LApps: Technological, Legal and Market Potentials of Blockchain Lightning Network Applications* (Mar. 2019) 185–89, available at https://dl.acm.org/citation.cfm?id=3325942 [hereinafter: *LApps*].

199. *Id.* at 186.

200. *Id.*

transaction fees.[201] Once such a channel is established, unlimited transactions can take place between the interacting parties.[202] Only the netted balance—once the channel is closed or both the parties cease to transact—is broadcasted to the base layer DLT network for consensus as a single transaction, which is subject to validation and verification by the DLT nodes.[203]

Lightning networks allow secure routing of transactions between two parties who are not directly connected by any point-to-point channel using secure "onion style" routing across multiple P2P channels.[204] In ordinary routing, the packet contains the address of the final destination and the next hop address.[205] The intermediate hop—usually a router or switch—replaces the next hop address every time the packet passes through them, based on the path determined by the routing algorithm used.[206] Thus, the final destination is known to everyone, although the message itself—the transaction data—would remain secure because it would be protected by end-to-end encryption.[207] In onion style routing, the path of the transmission is pre-determined and layered like an onion.[208] Each intermediate node will peel off one layer to exclusively find the next hop address. Only when the deepest layer is peeled off will the final destination—the recipient hop/node—become visible.[209]

Since first being successfully implemented, the lightning network has been used in an exponentially increasing number of applications—thus automatically expanding the scope of indirect channels.[210] Since July 23, 2019, over 4,000 of the roughly 9,000 "reachable" nodes in the Bitcoin network were lightning network enabled, generating 32,588 channels with a network capacity of 904.04 BTC for transfer.[211] The original form of lightning network now has several variant implementations, based on recommendations received from the

201. *Id.*
202. *Id.*
203. *Id.*
204. *Id.*
205. *See id.* at 186.
206. *See id.*
207. *See id.*
208. *See id.*
209. *See* Real-Time Lightning Network Statistic, https://1ml.com/statistics (last visited Oct. 23, 2019).
210. Miraz & Donald, *LApps*, *supra* note 198, at 186.
211. *Id.*

developers of the Bitcoin community.[212] While similar applications, such as Ethereum's Raiden Network, have been developed, the lightning network is still considered to be the most technologically advanced two-layer off-chain solution utilizing HTLC-based smart contract.[213]

We propose use of lightning networks in a DLT network for securities trading and settlement in order (1) to achieve the latency necessary for the real-time synchronization of bid/ask queues from order-matching platforms and (2) to allow broker-dealers to change their positions during an intra-day period prior to actual settlement. Information is crucial to the operation of securities markets, and the network protocol can be designed along the following lines to ensure proper channeling of information:

> 1. Confidential data transmission tête-à-tête will be permitted between transacting parties using onion style routing to communicate broker-dealer trading history and asset positions to order-matching platforms.
>
> 2. A public broadcast of data through ordinary routing would be used for communication of the bid/ask queues to the network participants.
>
> 3. Different types of information would be known only to select nodes to ensure that confidential trading strategies are not broadcast to the network. This can be implemented either by onion style multicasting or by traditional multicasting. In both cases, the same packet is to be sent to selected final destinations, such as evidence of transactions in a given security sent to issuers at end-of-day for purposes of settlement.

In the market structure model proposed here, lightning networks would be used to (i) give every broker-dealer of the DLT network an instantaneous copy of pre- and post-trade pricing information from the order books of all matching venues, (ii) feed all order-matching platforms real-time information about the cash, assets and trading positions of each broker-dealer node within the DLT network for risk management purposes, and (iii) allow broker-dealers to place orders on any platform and hold their matched trades on the second layer intra-day, freeing them to enter or exit any position during the trading day and

212. *See* Donald, *Bridging Finance*, *supra* note 17, at 185–86.
213. Miraz & Donald, *LApps*, *supra* note 198, at 186.

prior to actual settlement, at which time the transactions would be memorialized in the underlying ledger.

III. CONFIGURING A DLT NETWORK FOR SECURITIES MARKETS

A. WHY AND HOW TO CHANGE THE EXISTING MARKET STRUCTURE

As discussed in the introduction to this Article, the currently dominant model for securities markets can be considered efficient if one accepts the fragmentation of pricing and disruption of ownership that significantly impair the rights of investors, issuers and smaller broker-dealers. On the other hand, if a securities market were to be based on DLT, the basic structure of the protocol would make identical information available to every node, although such access could be intentionally segregated to preserve confidentiality, as explained below. The main argument against using a DLT network is its famously high latency, but as explained in Part II, *supra*, this can be reduced to current market speed through use of a private network combined with a layer 2 lightning network.

The primary concern remaining is then to decide whether the current state of the market justifies a major infrastructural change.[214] To decide this fairly, it is necessary to recognize how costs and benefits are currently compared: the present model puts its costs on issuers, investors and smaller broker-dealers—who have little influence over infrastructure design— while yielding benefit for the largest market participants who control the design process.[215] Moreover, as Mainelli and Milne point out, restructuring the market with DLT presents "substantial (although as yet unquantified) costs in the short to medium term while the anticipated benefits lie largely in the relatively distant future."[216] Incurring cost today in order to enjoy benefit tomorrow is not a virtue readily practiced in contemporary society, as anyone working on climate change or pension systems can explain.[217] Yet, when a specific structural evolution can bring wide-spread benefit but is blocked by powerful interests extracting rents from existing

214. Mainelli, *supra* note 14, at 6.

215. Throughout history, from the first stock exchanges to the most recent audit trails and matching portals, infrastructure is designed and implemented by leading broker-dealers. This history is examined in *Block Lords*, *supra* note 20, at 38–45.

216. Mainelli, *supra* note 14, at 6.

217. *See id.* at 25.

inefficiency, the matter is ripe for regulatory intervention.[218] Embedded benefits for larger broker-dealers argue strongly against their unbiased leadership to promote fundamental overhaul.[219] Negative system externalities borne by issuers and investors and competitive disadvantages borne by smaller broker-dealers argue for a regulatory intervention.[220]

We are not alone in advocating a realignment of securities markets towards the interests of issuers and investors. Mattli marshals a book-length study to advocate "a simpler and more transparent marketplace that better serves the interests of investors than today's opaque and highly fragmented markets," although he sees it arising from a natural consolidation of exchanges.[221] Micheler and van der Hayde argue, as we do, that securities settlement should be more transparent and less oriented toward the interests of financial intermediaries.[222] However, they do not yet examine in detail how DLT will achieve this, stating, "let us assume for the purpose of this article, that computer science can deliver an un-intermediated ledger allowing investors to hold and transfer securities and money in real time."[223] Avgouleas and Kiayias also make a similar political economic argument against rent extraction by market structure controllers, but in discussing the application of DLT, limit themselves to pointing out generically how DLT could shift some of the volume of derivatives clearing to the DLT network, diminishing the importance of the CCP.[224] The same argument could be made for using multiple global depositories rather than a CSD *cum* CCP.

The very significant impediment to straightening out the markets so that they best serve the interests of all constituencies is, as Mainelli and Milne observe, that achieving "substantial potential gains of using

---

218. *See id.* at 52.

219. MATTLI, *supra* note 5, at 168.

220. Eva Micheler & Luke von der Heyde, *Holding, clearing and settling securities through blockchain/distributed ledger technology: creating an efficient system by empowering investors*, 11 THE BUTTERWORTHS J. OF INT'L BANKING AND FIN. L. 652, 652–53, 655 (2016).

221. *Id.* at 653.

222. *See* Emilios Avgouleas & Aggelos Kiayias, *The Promise of Blockchain Technology for Global Securities and Derivatives Markets: The New Financial Ecosystem and the "Holy Grail" of Systematic Risk Containment* 34 (Edinburgh School of Law Research Paper Series, Working Paper No. 2018/43, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3297052.

223. Mainelli, *supra* note 14, at 12–13, 36.

224. *See* Avgouleas & Kiayias, *supra* note 222, at 33–34.

mutual distributed ledgers in settlement" will require both "coordinated and widespread change in operational processes across all the major public markets" and "a substantial reengineering" of existing arrangements.[225] Such reengineering on behalf of system outsiders has occasionally been successful in the past on a limited scale, such as in the founding of IEX to help institutional investors limit the damages inflicted by high frequency trading.[226] Any such reorganization of markets, however, must understand the numerous and interconnected, deep structural problems in the current system and ensure that they are not merely shifted into an automated existence through "network protocol" of a future DLT-based system.[227]

If a DLT-based settlement framework could conquer "fragmentation" and obviate "indirect holding," its introduction would bring sorely needed improvement to the financial system.[228] To achieve this, the bid/ask queues of disparate order-matching platforms would have to be replicated in a dispersed manner, and the settlement system would have to return the sole power to create securities to the issuers.[229] The permissioned DLT network we propose to achieve this would have three different and distinct types of nodes with three different types of information and authority: order-matching platforms, broker-dealers, and securities issuers. It would thus be very different than the self-sufficient and mostly egalitarian Bitcoin blockchain.[230]

A concentration of liquidity would arise from the nature of the DLT network itself because in a distributed ledger, each node holds a complete copy of the ledger.[231] The greatest weakness of having multiple platforms match trades in a given set of securities is that each platform develops an isolated set of price data that inevitably deviates

---

225. *See* Mainelli, *supra* note 14, at 36.

226. *See* Investor's Exch., LLC, Exchange Act Release No. 34-78101 (June 17, 2016).

227. Ensuring that any existing, imbedded advantages for leading broker-dealers continue in a future DLT network is exactly what major consortiums of banks now developing DLT for the financial markets will work to achieve. That is why independent scholarship on the topic and regulatory vigilance regarding market infrastructure is of such importance.

228. *See* Joseph Lee, *Distributed Ledger Technologies (Blockchain) in Capital Markets: Risk and Governance* 9 (May 18, 2018), https://ssrn.com/abstract=3180553.

229. *Id.* at 6.

230. *See* Miraz & Donald, *Atomic Swap*, *supra* note 138, at 42.

231. Lee, *supra* note 228, at 9.

from those of other platforms. If trades are conducted on separate venues which are all nodes of the same DLT network, this fragmentation would not arise, although the platforms could still compete on their fees.[232] As discussed below, the latency of the synchronization process would be dramatically reduced by running the matching system on a second, "lightning" layer of a permissioned network. Under the network protocol, matching platforms, as nodes of the DLT network, would be given full authority over the creation of matched trades.[233]

Transparency of ownership would be the immediate result of returning securities to the issuers' books and no longer treating them as something endogenous to the financial system.[234] Transparent ownership is already provided for in existing corporate and commercial law.[235] The laws governing both corporations and registered instruments—whether shares or debentures—give investors legal title to and status under the instrument purchased through registration of the owner's name.[236] But a settlement system that governs such instruments by full application of corporate and commercial law, rather than depository account rules or hybrid rules designed for the latter—i.e., "security entitlement" provisions—would enable investors to once again become fully empowered and visible owners.

The operating protocol of a DLT network designed for dependence on the real-world origination and ownership of securities could not be one that independently determines the creation of securities the way it does for Bitcoin. In the permissioned system proposed here, issuers would be given final authority over the creation and transfer of securities traded in the DLT network.

Other important changes would result from the proposed restructuring, in particular with regard to risk management. As already mentioned, the various functions of the system—as well as the given

---

232. *See id.* at 11.

233. Del. Code Ann. tit. 8, § 219; U.C.C. § 3-109(b) (AM. LAW INST. & NAT'L CONFERENCE OF COMM'R ON STATE LAW 2018).

234. *See* U.C.C. § 8-106 (b)(2) (AM. LAW INST. & NAT'L CONFERENCE OF COMM'R ON STATE LAW 1994); AM. LAW INST. & NAT'L CONFERENCE OF COMM'R ON STATE LAW 2018, Prefatory Note U.C.C. Art. 8 (2017).

235. *See id.* §§ 8-115 cmt. 3, 8-503 cmt. 3 (1994); AM. LAW INST. & NAT'L CONFERENCE OF COMM'R ON STATE LAW 2018, Prefatory Note U.C.C. Art. 8 (2017).

236. For corporate law see *e.g.*, Del. Code Ann. tit. 8, § 219. For the law of negotiable instruments see *e.g.*, U.C.C. §§ 3-109(b) (AM. LAW INST. & NAT'L CONFERENCE OF COMM'R ON STATE LAW 2018).

latency constraints of public networks—would demand that the DLT network be private/permissioned, perhaps operated by a federation of leading trading venues, broker-dealers, and issuers.[237]

The addition of a layer 2 lightning network should bring processing speed up to a level at which order-matching platforms could automatically scan and analyze the trading, cash, and asset positions of broker-dealers before executing orders.[238] This would allow the market's risk management mechanism to operate prophylactically, rather than post hoc, through a CCP designed merely to contain the blast of default. While such use of the DLT network to perform CCP risk management functions does not go as far as the extension into smart corporate and regulatory compliance mechanisms suggested by Lee, its pre-emptory nature does improve upon the current technique of absorbing default.[239]

The model proposed here would thus (i) give order-matching venues power to reject an order if its originator shows an insufficient asset position, (ii) empower the network protocol to block and extract assets for purposes of execution and settlement, and (iii) use a smart contract risk allocation arrangement among broker-dealers to absorb the impact of defaults that escape preventative screening.

The following subsections examine the manner in which a DLT-based securities settlement system can be used to reconstitute unified pricing across the market, restore transparency of asset ownership, and reduce settlement risk.

B. Overcoming Fragmentation of Liquidity and Information

Liquidity is directly linked to network externalities, so that a higher number of buyers and sellers actively engaging in procurement and disposal of assets on a given order-matching venue will generally lead to higher liquidity.[240] A similar relationship exists for transparency and information: the more information that can be grasped from a given standpoint, the higher the level of transparency.[241] If all order-matching platforms active in a market are made nodes in that market's DLT

237. On the available governance mechanisms for a DLT network see RAUCHS ET AL., *supra* note 1, at 55–56.

238. *See* Lee, *supra* note 228, at 14.

239. *See id.*

240. *See* Hans. R. Stoll, *Future of Securities Markets: Competition or Consolidation?*, 64 FIN. ANALYSTS J. 15, 15–16 (2008).

241. *See id.* at 20.

trading and settlement network, the bid/ask queue maintained by each platform would be distributed within the identical copies of the ledger maintained by all other nodes in the network.[242] The distributed nature of the technology constituting the framework on which communication and matching of orders is based would itself unify pricing data and overcome market fragmentation.[243] One might even consider linking multiple markets—such as equity and futures—on a single DLT network.

Today, market participants demand that trading be as close as possible to instant, which makes latency crucial. Orders should be transmitted, read, and executed instantly, and post-trade data showing execution price should also be instantly available. This can be achieved by hosting each order-matching node on a layer 2 lightning network, which is capable of providing latency as low as existing, non-DLT technology. The layer 2 would still enjoy the cryptographic protection of public and private keys, but would not suffer from the time-consuming consensus process.[244] This will not be problematic, as it will be within a private/permissioned network in which nodes have assigned authorities.[245] Although data updated to the millisecond—rather than the microsecond—may not meet all needs of high frequency traders, it should be satisfactory for most market participants and for regulators, who would receive much better information than proposed to be available through the CAT, for which T+1 aggregation of data to the regulator is the goal.[246]

C. TRANSPARENT HOLDINGS THROUGH DLT

Securities, whether shares of stock or debt instruments, come into existence when issued by the entity against which claims embodied by the securities may be exercised.[247] The issuing entity or its agent are responsible for recording the securities' existence, which takes place under either corporate law or contract law, depending on whether shares

242. Lee, *supra* note 228, at 13.

243. *See* Stoll, *supra* note 240, at 18.

244. *See* Mainelli, *supra* note 14, at 14.

245. U.C.C. § 8-103 cmt. 2, AM. LAW INST. & NAT'L CONFERENCE OF COMM'R ON STATE LAW 1994); AM. LAW INST. & NAT'L CONFERENCE OF COMM'R ON STATE LAW 2018, Prefatory Note U.C.C. Art. 8 (2017).

246. *See* 17 C.F.R. § 242.613(c)(3) (2016).

247. *See* Lee, *supra* note 228, at 6.

or debt are being issued.[248] This genesis is very different from that of a cryptocurrency unit, which comes into existence when nodes comply with rules embedded in the protocol of its native DLT network.[249] It is also very different from the permitted creation of securities through book-entry in the indirect holding system.[250]

Securities traded or settled on a DLT network could not be fully network-endogenous without giving the network protocol free reign to create these securities.[251] Thus, securities traded on a DLT network should originate according to an authority exogenous to the network protocol, that is, the records constituting their existence must not be determined by the network alone.[252] The challenge for any securities settlement system aspiring to utilize transparent ownership is to allow ownership records to be held authoritatively by the issuer while simultaneously permitting such records to be altered by a robust transfer of title at low latency in connection with market trades.[253] Some ideas currently aired about how securities settlement could work on DLT appear to assume that the DLT network would control the creation of securities just as the Bitcoin blockchain controls the origination of Bitcoin and securities intermediaries currently control the creation of

248. Under each of the U.S. corporate law statutes, shares exist, and shareholding must be entered, in a register of shareholders. See Donald, Darkness, *supra* note 29, at 61–62. Debt issued as a negotiable instrument (i.e., bonds or debentures) are contracts for debt, and if the instruments are not offered to the public there is no need to create a trust indenture arrangement, although it is difficult to imagine that the company would not keep some sort of central register of bond- or debenture-holders.

249. An ordinary Bitcoin transaction comprises of two major components: valid unspent input(s) and valid out(s). Let us consider a scenario where A receives 2 and 3 BTC respectively from B and C and would like to transfer 5 BTC (from the received transactions) to D. The unspent transaction outputs from B and C can now be used as inputs for new transaction to be made to D. However, there is especial arrangement for "Coinbase" transactions—the creation of new BTC. Analogous to "genesis block," a "Coinbase" does not have any input parameters. Miners, when completing the PoW puzzle, includes a "Coinbase" transactions with an output to himself or herself equivalent to the Bitcoin mining reward rate of the time of creation which is 12.5 BTC as of now. Successful completion of the block, subject to consensus, thus creates the new supply of coins.

250. As noted above, under U.S. law this would be the "security entitlement" invented by the Uniform Commercial Code. *See* U.C.C. §§ 8-501, 503 (AM. LAW INST. & NAT'L CONFERENCE OF COMM'R ON STATE LAW 2018).

251. *See* RAUCHS ET AL., *supra* note 1, at 41.

252. *See id.* at 47, 51.

253. *See* Mainelli, *supra* note 14, at 24–25.

shadow securities by book-entry "security entitlements." If such a model were implemented, the distortions of ownership and transparency caused by the indirect holding system would be perpetuated.[254]

To achieve transparency and restore property rights, traded securities should exist as "uncertificated securities" on the books of the issuer, and the purchasing broker-dealer should have authority to instruct the transfer to its name or the name of its client upon presenting evidence of a confirmed trade executed within the DLT network. The ultimate transfer would take place only on the books of the issuer (its register of shareholders or bondholders). The book-entry of an uncertificated security in the name of its owner constitutes full and negotiable transfer for purposes of commercial law and would create full and transparent entry of ownership for purposes of corporate law or the laws governing relations among bondholders.[255]

D. An Initial Model for a DLT Network

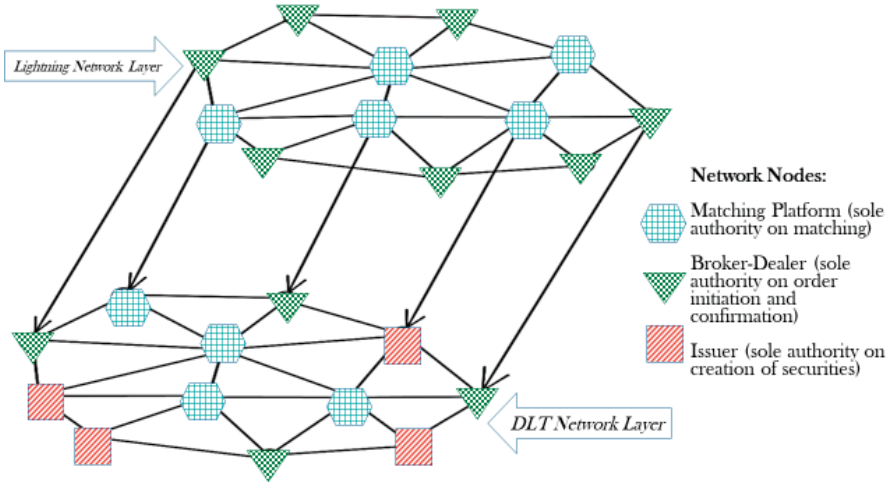
As outlined in Figure 4 below, a DLT network could be used as the base infrastructure for a securities market in which order-matching platforms, broker-dealers, and issuers are nodes. The network would have two layers, one consisting of the underlying DLT and a second consisting of a lightning network. The order-matching platforms as nodes of the DLT network would also operate on the lightning network, which would allow both their instant receipt of the asset positions of broker-dealer nodes and the replication of all bid/ask queues. Broker-dealers would have to report cash and security account data to the lightning network and have authority to initiate and confirm trades on the lightning and underlying networks. They would receive information only about their own positions and the existing queue, with no access to the trading history or asset positions of competitors. Issuers would be nodes of the DLT network with ultimate authority to register the existence and transfer of their own securities. They would receive information on matched trades in their securities for end of day settlement on the underlying ledger.

---

254. *See* Lee, *supra* note 228, at 1 ("[DLTs] have the potential to revolutionise securities trading . . . through removing reconciliation and other costs that are no longer needed with the trust and transparency DLT brings.").

255. *See* U.C.C. §§ 8-501, 508 (Am. Law Inst. & Nat'l Conf. of Comm'r on St. L. 2018).

Figure 4



The overall system as sketched out in Figure 4 would require:

(i) A private/permissioned DLT network in which order matching platforms, broker-dealers and issuers are nodes with different roles, authorities and information received;

(ii) Network protocol and design would be controlled by a private federation, probably of leading broker-dealers, matching platforms and issuers;

(iii) The broker-dealers would have authority only to make orders and confirm transfers;

(iv) The order-matching platforms would have authority only to match, or refuse to match, orders into a trade, creating a claim against the seller for securities and a claim against the buyer for cash;

(v) The issuers would have sole authority to create securities and register the transfer of the same on the ledger, pursuant to the consensus confirmation of broker-dealers;

(vi) Banks would remain outside of the DLT network but be connected to report cash balances of participants and by smart contracts triggering disbursement of cash in connection with verified and confirmed trades as well as loss allocation payments;

> (vii) Registration of transfer and release of cash would happen simultaneously pursuant to the DLT network protocol upon confirmation at end-of-day, creating strict delivery versus payment (DvP).

The system would have to be Turing-complete in order to support smart contracts.[256] If crypto assets are to be accepted as an alternative to cash, the system should also include HTLC or lightning network facilities supporting atomic swaps between the cryptocurrency network and the securities trading network.[257]

In the proposed model, each matching platform would run an order-matching engine that applies the standard "price-time priority" matching algorithm, just as in existing exchanges.[258] Instead of being novated into twin contracts through insertion of a CCP, the matched trade would be fed into the DLT network for end-of-day settlement. Institution identifiers used in the order submission and order-matching system to track buyer and seller would translate into identifiers on the DLT network. The "escrow" function of the CCP—which has access to funds and can guaranty payment—would be performed by the protocol of the DLT network, which would earmark funds and securities for delivery. The information fed over the lightning network to each order-matching platform for risk management purposes would include the reduction of available assets and cash stemming from such current trading. Implementation of the proposed DLT framework would thus not only obviate the U.S. CAT project and the EU need for consolidated tape providers with respect to pricing data, but it would also bring derivative-market-quality risk management to the equity market.[259]

Every broker-dealer node of the DLT network for trading and settlement would have to register securities and cash accounts within the

---

256. "Turing completeness" is the power of any device or system to emulate a Turing Machine, i.e., the capability of data-manipulation rule set (such as a computer's instruction set, a cellular automaton or a programming language). *See* RAUCHS ET AL., *supra* note 1, at 51.

257. However, these technologies are still in their infancy and much improvement is required before they can be used in a large-scale system. In fact, both traditional banking system and atomic swaps for crypto assets can be applied in parallel. *See* Miraz & Donald, *Atomic Swap*, *supra* note 138, at 48.

258. That is, best price is matched first and if two orders bid or ask the same price, then first to arrive in the system is matched first. *See* SCHWARTZ & FRANCIONI, *supra* note 3, at 164.

259. *See* Donald, *Block Lords*, *supra* note 20, at 34.

network. This is identical to what is now done on securities exchanges, and from a functional point of view would be similar to a multi-signature "wallet" used in a cryptocurrency exchange. This information would be held at the level of the lightning network and be visible to every order-matching node to which such broker-dealer is eligible to submit a buy or sell order. This information would not be visible to other broker-dealers or issuers. The information would allow the order-matching node to verify the existence of assets prior to matching, serving a gate-keeping risk management function, while shielding it from use by competing traders.

Because the bid/ask queue of each order-matching venue would be held on the lightning network, pricing information on any asset sold on many such venues would be instantly consolidated, eliminating fragmentation of price discovery. The lightning network would temporarily record each matched trade, making it available for broadcast to the other broker-dealer nodes for consensus and incorporation into the DLT settlement network at end of day. The transfer of ownership rights recorded on the lightning network is bi-directional and thus transfers could be performed an unlimited number of times before the channel is closed at end of day, which would allow traders to enter and exit an asset as often as they like before close of trading, at which point only the net result would be fixed, broadcast, and registered. At end of day, the lightning channel would close, and the broker-dealers' final balances would be broadcasted to the network nodes for consensus and registration in the base ledger. Funds and securities would then be delivered definitively through the network by entry into the relevant registers and accounts.

It is important to make trade commitments immediately visible without requiring every participant to settle its trades immediately.[260] Immediate delivery does not correspond to the wishes of most market participants, and because some early DLT proposals for securities settlement included such immediacy they were deemed undesirable.[261] Securities trading does not have the sole purpose of obtaining actual delivery and long-term retention of securities. Harvesting price changes intra-day may be the sole target of most trades. Attempting to eliminate

260. *See* Avgouleas & Kiayias, *supra* note 222, at 52.

261. This reality of markets is pointed out by Mainelli, *supra* note 14, at 14, who also observe correctly that the legacy securities settlement framework also allows near real-time settlement.

such "speculative" trading would be an unacceptable, normative intrusion into the nature of securities markets.[262] It is all but impossible to separate speculation from investment, despite history's best efforts to do so.[263]

With current arrangements for end-of-day settlement or batch settlement intra-day, and rules allowing T+2 or T+3 settlement, traders can be in and out of an asset hundreds of times before actually having to pay out cash or deliver securities.[264] This agile character of securities markets is something neither broker-dealers nor institutional investors would want to give up. To address this, in our proposed model, settlement—i.e., delivery of cash and securities through consensus of ledger nodes—would occur only when full confirmation through consensus occurs at end of day (or at the close of another specified cycle), triggering transfer of assets on the ledger at that time. Thus, purchase of a given security at day's open would earmark cash necessary for that purchase in the DLT lightning network, but a sale of that same security at midday would adjust the balance, perhaps indicating a cash credit for the broker-dealer who was in and out of the asset.

Lightning networks could thus allow order-matching platforms to assume a risk management role similar to a CCP in addition to allowing the pricing data held by these platforms to be aggregated in real time without asking market participants to fundamentally reform their approaches to securities trading. Because the lightning network transactions would not be permanently recorded in the ledger, a function comparable in some ways to the current system of netting could also be achieved, as the actual delivery activity could be substantially less than

---

262. *See* JOHN MAYNARD KEYNES, THE GENERAL THEORY OF EMPLOYMENT, INTEREST AND MONEY 260 (1936).

263. The desirability of eliminating "speculative" trading has been discussed long and often without approaching resolution. *See* JOHN MAYNARD KEYNES, THE GENERAL THEORY OF EMPLOYMENT, INTEREST AND MONEY 101 (1936) ("Speculators may do no harm as bubbles on a steady stream of enterprise. But the position is serious when enterprise becomes the bubble on a whirlpool of speculation"). Current efforts focus on transaction taxes, which would essentially allow traders themselves distinguish between trades they find necessary and unnecessary in light of the tax cost per trade. *See* Richard Rubin, *Democrats Aim for Financial-Transaction Tax*, WALL STREET J. (Mar. 5, 2019), https://www.wsj.com/articles/democrats-aim-for-financial-transactions-tax-11551818240 [https://perma.cc/8H53-ZRVW].

264. Mainelli, *supra* note 14, at 27.

the trading activity. The settlement at end of day would occur under a strict rule of delivery versus payment (DvP). As in current systems, participants would have cash accounts linked to the DLT network, and the ledger protocol would be coded with a function to confirm availability of funds. Both securities and funds would remain network exogenous, even when transferred to the seller's account.

However, the system could also be designed to allow cryptocurrency or other colored tokens as a medium of payment. In such cases, atomic swaps—preferably powered by HTLC and a lightning network—can be applied to confirm the availability of required funds instead of using third-party guarantors such as banks.[265]

The actual delivery of securities in fulfillment of trades would be a key improvement of the DLT model. Transactions would be received from the matching engine and broadcasted to the broker-dealer's party to the transaction and the issuer of the relevant securities as nodes of the network. Participating broker-dealers, which would be system nodes in this permissioned network, would perform consensus verification of each received contract and ensuing transfer through an automatic reconciliation of their trade records and the data broadcast to the settlement system at end of day.[266] This consensus verification would be limited to actual transfers to be settled and would not require that the trading history of any broker-dealer be made known to the market. Validation of transfer would trigger release of buyer's funds. Once a transfer of securities is validated and confirmed, the transaction would be broadcast to the DLT network for definitive registration in a process undertaken by the issuer.[267] Although the issuer would undertake such

---

265. *See* Miraz & Donald, *Atomic Swap*, *supra* note 138, at 43; *see also* Miraz & Donald, *LApps*, *supra* note 198, at 187.

266. While we are proposing end-of-day settlement, there is no reason why the same system could not operate on "batches," perhaps at mid-day, end-of-day and evening, or even on eight-hour cycles, if this were made necessary by trading hours.

267. Alternatively, similar to "Coinbase" transactions in a permissioned DLT system for securities settlement, the protocol could be designed so that the authority to create (issue) new shares by booking them on the main DLT trading network itself can be assigned to issuers as designated party, without consensus or external approval. This would address the problems associated with over-issued "shadow" securities created by intermediaries and depositories, but would unnecessarily distance the power to transfer securities from the transactions necessitating such transfer. We see the checks and balances arising from broker-dealer consensus *together with* issuer authority over the ledger change as better promoting transparency and avoiding moral hazard arising from conflicts of interest.

registration, it would be required by the network protocol. As such, the issuer would not be in a position to refuse transfer.

The trading and settlement system would therefore have four layers: (i) a central connecting DLT network operated by all participating broker-dealers, (ii) order-matching platforms receiving information on all broker-dealers submitting orders, (iii) a cash transfer system, and (iv) network nodes controlled by issuers on which securities originate and reside. As discussed above, the securities would thus remain exogenous to the primary settlement network, residing as uncertificated securities in a register controlled by the issuer. This register could be changed only with permission of the relevant listed issuer, which would also have the sole power to create any new shares through lawful issue. The securities traded would exist electronically and only in one place, so there would be no need to double- or multiple-book "shadow" securities within the broker-dealers' accounts.[268] The sole register in which the securities exist would allow complete transparency of ownership.[269]

E. SHIFTING CCP FUNCTIONS INTO ORDER-MATCHING PLATFORMS

As noted above, an additional benefit of the proposed model would be the ability to shift the risk management functions of CCPs to order-matching platforms, thus making this function preventative rather than remedial.[270] In order to achieve this, order-matching platforms would need to receive the day's trading history and asset positions—cash and securities—on every broker-dealer that submits an order. This would be similar to the information received by the CCP of a derivatives

---

268. As Martin points out, once securities are truly dematerialized and exist only in registered form, any secondary or tertiary accounts containing booked claims referring to the original account booking are unnecessary and dangerous, risking the creation of securities that have no validity. Martin, *supra* note 71, at 70.

269. It should be noted that we are referring to voluntary transparency, that is, transparency which is not destroyed automatically by the market infrastructure. The choice of a given shareholder to register ownership in the name of a trust or use an anonymous investor identifier would remain possible under our proposed model, and the desirability of such actions for tax or other purposes goes beyond the range of this paper. On this last topic, see Delphine Nougayrède, *Towards a Global Financial Register? The Case for End Investor Transparency in Central Securities Depositories*, 4 J. OF FIN. REG. 276 (2018).

270. *See* Avgouleas & Kiayias, *supra* note 222, at 8.

market.[271] Given the properties of lightning networks, delivery, and processing of this information should be possible within acceptable latency for a securities market. The "processing" in question would be an automatic assessment of risk, and a rejection of any order whose execution entails a risk profile outside of the acceptable parameters set at start-of-trading—and perhaps adjusted intra-day—for the matching engine.

The proposed model contains obvious advantages. Even with all its power and financial backing, the CCP on a contemporary stock market can only react to and absorb the default of system participants on their obligations to perform existing contracts, stemming systemic risk through its extensive capital backing.[272] Risk management will be greatly improved by the introduction of an intelligent preventative gate, as is currently done with margin requirement adjustments on a derivatives exchange. Closing the door to questionable trades ex ante would not only eliminate risk preventatively, but also encourage trading participants to better monitor their asset positions on a running basis rather than collapsing and having the force of their default blunted by the CCP through bulk of its "unlimited" funds.[273] In the proposed DLT network, the order-matching platforms would add a screening of risk management derived from the trading and asset position of broker-dealers to their standard "price and time" algorithm, matching those with acceptable positions and rejecting others. Knocking an order with insufficient backing out of the queue would allow the trading system to replace currently remedial damage reduction with preventative risk exclusion.

A final concern remains.[274] What if a broker-dealer has a large, undisclosed position in another market or off-market and a large loss for that broker-dealer occurs after the matching platform approves another trade on the DLT network? As this could not be dealt with by the preventative information feed within the DLT network, a traditional default containment backup like a CCP would have to be created. This could be achieved in a way essentially identical to the current guaranty

271. *See* RULES OF HONG KONG FUTURES EXCHANGE LIMITED 616-632A (2018), https://www.hkex.com.hk/-/media/HKEX-Market/Services/Rules-and-Forms-and-Fees/Rules/HKFE/Rules/fe_vi.pdf?la=en [https://perma.cc/S33D-BY92].

272. *See* Avgouleas & Kiayias, *supra* note 222, at 8.

273. *See* Lee, *supra* note 228, at 11.

274. We would like to thank Mathias Bock for raising and stressing this issue at a seminar we offered for the Hong Kong Law Society.

funds and risk allocation payments used to fund CCPs. Such payments are made by the network of broker-dealers acting as clearing participants, and can vary both in relation to the trading activity of the contributor and the source and dimension of the default.[275] In the proposed DLT network, a loss allocation agreement could be entered into by all market participants and enforced though smart contracts, so that in the case of default, payments as pre-agreed could be drawn in proper proportion from the cash accounts of the broker-dealer participants. This would function just like the current backing of a CCP, with the only difference being that the network of contributing participants would be unified by the DLT protocol rather than by a stock corporation acting as CCP.

F. Increasing Direct Holdings Decreases the Quantum of Netting

Part I.D explained that the high proportion of transactions currently netted out in traditional securities settlement systems corresponds to the high proportion of securities legally owned by apex institutions within the securities market. If 99 percent of securities are held in custody by a CSD, then 99 percent of transfers could take place between the accounts of participants in the CSD, and it will be possible to net out crossing obligations among those participants, thereby dramatically reducing the number of actual deliveries necessary at the apex of the system.

Claims by lower level investors against the CSD's participants and their client local brokers, however, will still have to be established and documented, although these transaction costs do not currently count as "settlement" because the lower level investors never actually own the securities. This means that the figure of 99 percent reduction of delivery costs is somewhat deceptive. In a market where each investor actually owns securities rather than holding an indistinct claim against upper level institutions, netting would be dramatically be reduced. Only mutual and fungible obligations can be netted, so a greater number of actual owners results in lower mutuality. Commonality of obligations

275. *See, e.g.*, Edwin Budding and David Murphy, "Design Choices in Central Clearing: Issues Facing Small Advanced Economies," 31 (Reserve Bank of New Zealand Analytical Notes series AN2014/08, Reserve Bank of New Zealand (2014)), https://www.rbnz.govt.nz/-/media/ReserveBank/Files/Publications/Analytical%20notes/2014/an2014-08.pdf [https://perma.cc/4K5F-Q72K].

would only remain among institutions engaged in high-volume proprietary trading. Ordinary investors would likely have no such commonality. Therefore, a reduction in declared netting volume should not be understood as a significant increase in actual transaction costs for the market.

With regard to actual transaction costs, because the proposal outlined here envisages settlement taking place on the ledger at end of day, traders could enter and exit an asset any number of times through trades on the lightning network intraday without performing on settlement. During the period between trade matching and asset delivery, the trade would remain off-chain in the second, "lightning" layer of the network discussed in Part II. By keeping securities trades away from the base layer of the DLT network until close of day, the lightning network would allow speculative trading with near-zero latency and minimal transaction fees leading up to settlement. This would reduce transaction costs by allowing traders to achieve a net effect—plus or minus any cash difference resulting from price changes—at end of day if they effectively reverse their positions. When the channel is closed at end of day, only the netted result of the transactions entered into by a market participant would be locked in and broadcast to the network for consensus.

CONCLUSION

Use of a DLT network for securities market infrastructure promises to solve the serious problems of fragmentation and disrupted ownership troubling markets today, both of which also prevent market transparency. These problems arise from the legacy infrastructure and its natural evolution away from physical trading venues to a constellation of electronic platforms. Although the market model used today is fast, secure, and cheap for the largest broker-dealers, its basic configuration seriously damages the interests of other constituencies in the market—including investors, issuers, and smaller broker-dealers.

The DLT network model proposed in this Article would allow disparate data gathered by a large number of matching queues to be aggregated into a copy of a ledger available to all nodes. The order-matching platforms acting as nodes of the DLT network could compete with each other without fragmenting pricing data, which would be synchronized automatically by the ledger protocol. In a private/permissioned network, the different participants in the trading

and settlement system could be given distinct roles and authority. Thus, the broker-dealers would be given access to bid/ask queue information, but not the trading and asset positions of other broker-dealers. The issuers of securities traded would also be nodes of the network with sole authority to create securities and power to effect transfer of securities to settle trades at day's end. The problem of "shadow securities" created by financial institutions booking securities to account would no longer exist, and ownership of the securities traded would be direct and transparent because evidenced only on the register controlled by the issuer of the relevant securities. Broker-dealers would continue to be the most active agents in the market, with sole authority to initiate orders to the order-matching platforms and confirm trades for transfer on the network to the issuer nodes.

Beyond solving the basic problems of fragmentation, ownership, and transparency, the proposed model could improve the current risk management functions now undertaken remedially by the CCP. A precondition of node membership for all broker-dealers would be to make assets and cash dedicated to trading visible to the system. On the basis of this knowledge and the day's trading history, each order-matching platform would screen for default risk while processing the standard price-time priority algorithm. In this way, risk management would become prophylactic rather than remedial. The DLT protocol would not share this risk management data with broker-dealers, and all trading participants would agree to pay in automatically apportioned guaranty funds if default occurs despite the preventative screening. Thus, existing remedial action would remain available, although its use would be much less probable.

A serious problem of DLT networks can be latency, which is often too high for efficient securities trading; this also renders the network incapable of adequate scaling. To address this, we recommend using a private network that obviates the PoW consensus process and employs a "lightning network" layer parallel to the DLT network, which would allow intraday functions to occur instantaneously. Information about orders queued and trades executed on all order-matching nodes would be synchronized via this lightning network. These contracts would remain on the lightning network and would be part of the data fed to the order-matching platforms intra-day, but as settlement would not be instantaneous, traders could reverse positions without limit until close of trading. At that moment, a close-of-day confirmation process through consensus would bring all standing contracts into settlement and transfer

of ownership on the registers controlled by security issuer nodes, making the transfers permanent records.

While a reorganization of this magnitude would be highly unusual in a system that works well for its leading broker-dealers, it would benefit investors and issuers and smaller broker-dealers. Given the manner in which markets are designed and built under the leadership of the largest market participants, regulators should perform their duty to protect the weaker constituents in the broader market and seriously consider implementing the more just and transparent arrangement that technology now allows.